IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
RICHMOND DIVISION

UNITED STATES OF AMERICA	)	
	)	Criminal No.
v.	)	3:19CR130
	)	
OKELLO T. CHATRIE	)	June 24, 2021

COMPLETE TRANSCRIPT OF ARGUMENT
ON MOTION TO SUPPRESS
BEFORE THE HONORABLE M. HANNAH LAUCK
UNITED STATES DISTRICT JUDGE

APPEARANCES:

Kenneth R. Simon, Jr., Assistant U.S. Attorney
Peter S. Duffey, Assistant U.S. Attorney
U.S. Attorney's Office
SunTrust Building
919 East Main Street, Suite 1900
Richmond, Virginia 23219

Nathan P. Judish, Assistant U.S. Attorney
U.S. Department of Justice
950 Pennsylvania Ave., NW
Washington, Virginia 20530

Counsel for the United States

Laura J. Koenig, Assistant Federal Public Defender
Paul G. Gill, Assistant Federal Public Defender
Office of the Federal Public Defender
701 E. Broad Street, Suite 3600
Richmond, Virginia 23219

Counsel for the Defendant

DIANE J. DAFFRON, RPR
OFFICIAL COURT REPORTER
UNITED STATES DISTRICT COURT

(The proceedings in this matter commenced at 10:10 a.m.)

THE CLERK: Case No. 3:19CR130, United States of America versus Okello Chatrie.

Mr. Kenneth R. Simon, Jr., Mr. Peter S. Duffey, and Mr. Nathan P. Judish represent the United States.

Mr. Paul G. Gill, Ms. Laura G. Koenig, and Mr. Michael W. Price represent the defendant.

Are counsel ready to proceed?

MR. SIMON: The United States is ready, Your Honor.

MR. GILL: The defendant is ready, Judge.

THE COURT: Well, thank you all. Obviously, we're here for argument. I want to be sure that you all know that you should proceed as you are comfortable with respect to COVID protocols. We have lifted largely most of what we're doing.

If you approach the lectern, please, I still think you should use our disinfectant in between speakers just out of safety.

All right. I'm ready to hear argument. Obviously, you have presented me with a good deal of information. So I'll hear what you have to say.

MR. PRICE: Good morning, Your Honor.

THE COURT: Good morning.

MR. PRICE: At issue in this case is a geofence warrant authorizing the search of numerous tens of millions of people without probable cause for a single one of them. It was a dragnet of epic proportions. A general warrant. The very thing the Fourth Amendment was designed to prevent.

It's obvious, or at least it should have been, that valid warrants don't look like this. There's a lot that's new about this case, but it's not new that a warrant must be supported by probable cause. It is not new that a warrant must be particularized.

So it's striking that this warrant leaves basic questions about what can be searched and seized up to Google and the government to work out, to play judge.

Good faith should therefore not apply. Valid warrants do not look like this. It was so profoundly overbroad, so lacking --

THE COURT: Sorry. I think you may have to be a little closer to the microphone. I'm sorry. Or pull it up. Yes, that's better.

MR. PRICE: I'm saying good faith should not apply. That this warrant was so overbroad, so

profoundly lacking in particularity that no reasonable officer could have relied on it.

As a result, Mr. Chatrie seeks this court to hold the warrant unconstitutional, to suppress the evidence obtained from it and all the fruits thereof.

I'd like to talk this morning first about overbreadth, then particularity, and good faith. First, I think it's very important to understand what happened here at the beginning when the initial search took place. When the government got a warrant compelling Google to search the account records of tens of millions of people. This was not something that Google normally does. It's not something that Google would have done absent the warrant. They were acting in this case as a government agent compelled by the warrant.

The search that Google did, the initial search of numerous tens of millions of people, is state action, no less than the seizure of the 19 accounts that followed or any of the steps, the warrant after that.

Google ads do not work this way. Google does not advertise and provide location information about its customers to advertisers. Google's advertising system doesn't sort through accounts in this manner.

The Sensorvault is, of course, not indexed according to location. It is indexed according to user account. And that is intentional. It's not that Google flipped a coin and decided to do it this way. It is irrelevant that they could have done it some other way. Here it is organized by user account because it is user data. It is not Google's business records.

It is not enough to simply cite statistics about Google's popularity or how many people have cell phones to establish probable cause for the kind of search that took place in this case.

There was not probable cause to search ten million user accounts. There wasn't probable cause to search 19 or 9 or even 1. There certainly wasn't probable cause to seize the account records of 19 people who happened to be nearby.

The Supreme Court has already weighed in on this, at least in the physical world. The idea that you can search people just because they are nearby to a crime was foreclosed by the Supreme Court in *Ybarro*, *Ybarro v. Illinois*. It said, "Mere propinquity is not enough. You must have probable cause with respect to each person searched and seized."

Here the government did not have probable

cause to seize all 19 accounts after the initial search.

THE COURT: Well, before you get there, I want you to explain to me how the fact that the tens of millions that were being searched were anonymized, they are not identified users, how that does or does not affect whether it's a search.

MR. PRICE: So, if you're talking about the numbers that were attached to each individual's account, those are unique identifiers that Google provided. So they're not anonymized for this time only. They are static identifiers associated with people's location history Sensorvault accounts.

So aside from the fact that it is possible to identify people based off of even a small segment of data, it would be trivial for the government in this case to obtain a subpoena, to go back to Google and to say, Okay, now please tell us the subscriber information for that anonymized number. They would not need to go back to a court to seek a warrant for that information once the Stage 1 data is turned over.

Those anonymized numbers associated with individual accounts, frankly, are not truly anonymous. It is very easy for the government to go back and get that information without a warrant just using a

subpoena for subscriber records.

THE COURT: Okay.

MR. PRICE: We would argue, Your Honor, that there was not -- we do argue that there was not probable cause to search or seize even one person's location history data in this case. There is no nexus between the robber and location history. There is some indication that the suspect had a cell phone, but there is no indication, certainly not in the warrant, that location history was enabled, something that only about a third of Google users have.

There was a -- if you take Google's view of it, there was a complex seven-step process that was required to enable it. We would say it was probably not that voluntary and knowing, but nonetheless, only a third of Google users have this enabled. So it is not enough to just say that the suspect had a cell phone. It's not clear if that suspect, that cell phone, was connected to Google. And it's not clear that that cell phone, if it was connected to Google, had location history enabled.

And, furthermore, given the uncertainty in Google's method of estimating location, there was at least another 32 percent chance that records would not be available, that somebody would be located outside

of that geofence.

So I think the percentage is certainly below 30 percent, even if you just take it by statistics. But we're saying that statistics are not enough here. There needs to be something that directly connects the warrant to the individual and the data being searched, that generalities or statistics about Google's popularity are not enough, that warrants must be -- probable cause must be individualized. And here it was not.

THE COURT: To be fair, at least some courts have relied on statistics at least to approve warrants in the past; is that right?

MR. PRICE: If you're speaking about the Illinois cases in particular, yes. One of the judges in that case looked at the statistics as an important factor in making that determination. But we argue, Your Honor, that statistics alone can never be enough, that there must be some individualized connection in each case. Otherwise, it would be simple for the government to recite those same statistics in every single case to say the facts of the crime, to say that there were cell phones involved, which is not much to accomplish these days, and that Google collects a lot of data, which is true. There would be no instance in

which the government couldn't obtain a geofence warrant.

That is why the Fourth Amendment requires that warrants be individualized, that proximate cause be individualized.

The government mentions the possibility of locating witnesses with the geofence warrant, but it is pure speculation that there were witnesses that the government had not yet identified. It seems that the most relevant witnesses the government would have already identified as being in the bank and/or through the surveillance cameras that they used initially, and that any additional witnesses found inside of buildings nearby or apartment complexes would, frankly, not have much to contribute. As one judge noted, they would have to be able to see through their walls, for starters.

The other thing I would say to that specifically is that the warrant is clearly focused on identifying a suspect, not on identifying witnesses. Witnesses are mentioned only once in passing in the context of some general information about how Google works. The clear focus of this warrant, the entire purpose of that three-step process, is designed to find the suspect, not to identify witnesses.

The same can be said of co-conspirators, which are never mentioned once in the warrant application. And, in fact, investigators knew that the suspect was seen alone coming to and from the bank based on the surveillance video.

So, once again, there are no facts to support this idea that the warrant was somehow being used for witnesses or co-conspirators in addition.

THE COURT: Well, they're saying there's not direct evidence, but they're saying because somebody was using a phone, it's likely while they were in the bank, at least there might be probable cause that they're calling a lookout.

MR. PRICE: I'm sorry?

THE COURT: That they are calling a lookout.

MR. PRICE: So, in this case, it appears that the government did an initial investigation and was aware that there wasn't another individual in the vicinity at the time. If that was the focus, it's not impossible that it --

THE COURT: So what makes you say they did the initial investigation and they knew there was not somebody there?

MR. PRICE: I believe Detective Hylton testified about the review of surveillance video they

did ahead of time, I believe it's in the CAST report as well, showing one individual leaving their car, going to the bank and back.

So if there was a concern that somebody else dropped somebody off or picked somebody up, that was already known at the time and most likely the reason the warrant is not seeking information at all about co-conspirators. They are not mentioned once.

So I think to argue that that was the point of this warrant and that there was cause for that just isn't supported on the record.

The whole point here, Your Honor, is that the government had no suspects. They were conducting a reverse warrant. They were starting with a bunch of data and trying to find a suspect based off of that. That is the reverse of how these warrants usually work when the government goes to Google and asks for information about a particular account or accounts or at least identifiable accounts. Here the whole process was turned on its head.

I'd like to shift gears to particularity, if Your Honor doesn't have any questions about overbreadth.

THE COURT: Well, I guess I want to confirm, a lot of your arguments point out that the breadth of

the search is quite overpowering and that there were other alternatives that the government could have done. Is there a legal requirement that the government use the less intrusive means to do an investigation?

MR. PRICE: No. There's no requirement that the government use the least intrusive means. I think it is different, however, to use a geofence warrant in the sense that it was more intrusive, but it is a way of trying to take a shortcut. There are, and were in this case, other avenues of investigation that the government could have pursued, traditional lines of investigation that they did not, and instead went to Google and said, "Google, tell us who robbed the bank." This was an easy way out in some sense.

THE COURT: So, Mr. Price, what I want to understand is why you're saying the shortcut is illegal. So there's no requirement for the least intrusive means. So, you know, one would hope that the government wouldn't waste resources in an investigation.

MR. PRICE: I see.

THE COURT: So what makes this illegal? It turns it on its head, but sometimes you turn something on its head and that's a good thing.

MR. PRICE: So there's nothing illegal about taking a shortcut per se, but this particular shortcut was so far afield from anything that any other court has signed off on. Certainly not the Supreme Court, not any circuit court, and there are now two different district courts, federal district courts, that have agreed that these warrants are unconstitutional. And so I think we're focusing not on the fact of a shortcut, but that this particular shortcut is completely unsupported by probable cause, and also fails the particularity requirement of the Fourth Amendment very badly at every step of the search.

Step 1, for example, goes back to this point about basic questions being left unanswered and left up to Google and the government to sort out. For example, which database to search: Location History, the Sensorvault versus Web & App Activity or Google Location Services. This was something that clearly the government had discussed with Google ahead of time, and they were both aware of which databases were going to be searched, but it wasn't in the warrant.

One reason it might not have been in the warrant is because that would require specifying that not all devices have location history enabled. So just saying we're going to search Google and Google

has location information about people makes it seem like everybody has this location information when, in fact, a third of Google users have this enabled.

So leaving out that fact wasn't a small thing. It very much dictated the overall scope of the search, which, of course, then led to tens of millions of people.

The warrant did not specify how to count if a device is inside that geofence. So we know, for example, from one of the Illinois cases, as well as the Kansas case that just came out, that the government is fully aware of this phenomenon of display radius extending beyond the geofence.

In fact, in two other cases at least, the government asked for -- explicitly told the judge that the display radius will extend beyond the geofence and that the government wants the data from everybody whose display radius even touched the geofence.

Another way to do it -- I should say that that method is likely to produce the largest number of false positives. If you are looking for anybody whose display radius intersects with that geofence in any way, there's going to be a high percentage that some of those people are going to never have been in that geofence at all. In fact, we know that happened in

this case in at least one instance where somebody was driving by and pulled in.

That's not the only way to do it. If you wanted to minimize the number of false positives, you could say, Return only the devices whose entire display radius is inside the geofence. And that would eliminate the possibility of false positives or at least drastically reduce it.

So there are multiple ways of going about this. And the government is aware of them. This warrant did not specify. And it left it up to Google and the government to sort out. The government says that Google correctly interpreted what they were intending, but none of that would be apparent to a magistrate looking at the face of this warrant.

It was likewise unclear what that geofence covers. There was no indication -- well, the government says that it was unusually specific because they identified a latitude and longitude and drew a precise circle around that, but that area is a congested urban area encompassing not just the bank, but a church and roads, at least, plus the businesses and apartments nearby that got swept in as a part of that effective range.

So we know that the effective range of the

geofence in this case was not 150 meters, that it was 387 meters, more than twice the distance of the original geofence, reaching not just that bank and the church, but Hull Street and Price Club Drive, Ruby Tuesdays, the Hampton Inn, A.M. Davis, Mini-Price Storage, the Genito Glen Apartments, and the Rockwood Village Senior Apartments. These are all places that were effectively covered by the search that the government requested here, none of which was ever signed off on by a judge or a magistrate.

The information presented to the magistrate showed a nice circle around the bank and the church and didn't mention the possibility that it would search people outside of that circle, and that the things outside of that circle that might be searched included apartment complexes, private businesses, a hotel. These are constitutionally-protected spaces. So that is significant.

And it is difficult to say that a warrant is narrowly tailored when most of the devices identified will have nothing whatsoever to do with the crime.

So even at Step 1, Your Honor, there were significant basic questions left unanswered, left to Google and the government to work out amongst themselves.

In some instances, maybe that arrangement had already been worked out, but it wasn't spelled out in the warrant. That's for sure.

Step 2 and Step 3 were far more explicit about the degree of discretion given to the government. Step 2 explicitly says that the government is going to narrow down the list and decide which people will have additional contextual location data revealed to the police. And that's the two hours total and wherever those individuals happen to go regardless of the geofence itself.

So it is at that stage completely up to the government to decide who to search, who to get more information from. Google pushed back. There was certainly a back and forth between Google here that illustrates this point very well, this negotiation between the government and Google over what is a reasonable amount of data to turn over in Stage 2.

But that is fundamentally a question that a judge should be answering, that should not be left, and cannot be left under the Fourth Amendment, up to the government to decide on its own.

Step 3 --

THE COURT: Well, before you get there, I have a question. So, with respect to Step 1 and the

identification of the 19, is there any dispute about how those 19 numbers were identified or how Google turned that information over to the government?

MR. PRICE: How it actually happened in this case?

THE COURT: Well, you're saying it got down to 19. So my question is, what is your position about how it got down to 19?

MR. PRICE: I see. So our position is that the search, the initial search, was of the numerous tens of millions of people. The 19 was the data seized from that search.

Now, there was a -- and I think is a question here that relates to particularity about how Google identified those 19 people. Google chose to say that anybody whose center points of their location -- so Google estimates location in a circle, and the latitude and longitude points are simply the center of that circle, wherever it happens to be.

The warrant in this case, the way Google interpreted it, was that anybody whose center point was inside the geofence was produced to the government as a part of that 19. I'm saying that there were other ways of going about doing that, which the government is fully aware of, and it just wasn't

spelled out one way or the other.

So one privacy protective way of doing this would be to say only return people whose display radius was entirely within the geofence. In other words, those would be much more precise readings perhaps because of GPS as opposed to Wi-Fi or cell-site location information. It would drastically reduce the number of false positives. And, as I mentioned once before, we know of one, and it's likely there are at least five in this case of those 19. So it wasn't -- this decision had consequences. And how you count who's in the circle matters.

And if it matters to determining how many sets of records you get to seize, then that's got to be something that is clear in the warrant to begin with. That can't be left up to officer discretion or Google's discretion down the road. And we make no distinction between Google and the government in this case. They are acting together, according to that warrant.

THE COURT: Is that what other courts have done?

MR. PRICE: So, the Illinois cases were decided. The opinions were issued there without the benefit of the record that we are here. And the

Kansas case, which was just decided, appears to be based on the records in the Illinois cases in terms of the factual records.

So one thing that those courts did not consider, perhaps because it wasn't known to them at the time, was the scope of this initial search that took place and how it differs, for example, from tower dumps or other types of searches.

I think had that information been known to those magistrate judges, that they would have perhaps at least paid some attention to that fact. It was just not before them. So I believe they were under the impression that Google was able to search records just in that location.

THE COURT: Well, I guess I was getting to your comment about agency. That Google and the government are -- you said Google is an agent of the government. Have other courts made that finding?

MR. PRICE: So, we do not argue that this is a private search. Google was -- which is that test for a government agent. Google was acting according to a warrant. It was compelled by legal process to assist the government; therefore, the government was not only aware of what Google was doing, but the government was directing what Google was doing.

And if Your Honor is looking for a cite on that, I would cite *Skinner v. Association of Railway Labor Executives* for the point that if you -- as the government requires, say, an employer, to conduct a drug test of their employees, that even though that's an employer, not the government, they're doing that testing at the behest of the government according to a statutory requirement, here a warrant, and therefore it is government action.

So I would say that what Google was doing here was government action. It was directed by the government.

Steps 2 and 3. Step 3, like Step 2, gave sole discretion to the government to decide which users would have their identifying information revealed. It is the same problem as in Step 2 in that the warrant explicitly gives this power to the government, which, of course, would have been obvious to the government as well as the magistrate who signed it.

There isn't a good response to that. And so the government's answer to it is that the whole three-step process doesn't matter at all, that this is just show, and they are, in fact, entitled to Stage 1, 2, and 3 data on everybody identified in that initial

geofence.

The problem with that is that it guts any argument that the three-step process has constitutional significance. And while it might take care of some of the particularity problems, it doubles the problems with probable cause. To say that no, the government actually had probable cause to search the information of all 19 people for two hours wherever they went, and to know exactly who they were, that is unsupportable from the facts. There is no allegation in the warrant or affidavit that other people that might be identified here were involved in the crime and would have evidence of criminal activity in their accounts. So it really does lay bare the probable cause problem if that's the answer to particularity.

It also would raise questions about whether a magistrate looking at this warrant would reasonably interpret that to be what it means. And so that is a relatively new argument the government has advanced, but I think if that is the route they choose to go, we would have questions about whether that's an accurate representation of what the warrant says.

Your Honor, the government also suggests that the warrant be severed and that perhaps Step 2 and Step 3 can be separated from Step 1. The problem with

severing in this case is that no part of this warrant was supported by probable cause. There is nothing to sever.

The de-anonymization doesn't matter for the reasons that I explained a little bit earlier, that it is possible to -- in fact, very trivial to identify people based off of those Sensorvault ID numbers with a mere subpoena. And that the whole process itself was nothing more than a fig leaf designed to obscure the magnitude of the search and seizure in this case.

If I can touch briefly on the question about whether this was a search. I know that that's something that the government has brought up as well. We certainly believe that *Carpenter* is the best analogy to this situation and that the Court should not try and rely on relics like *Smith* and *Miller*, outdated Supreme Court cases that are very far afield from the facts here.

Carpenter was concerned with information that reveals the privacies of life. Location history reveals the privacies of life just like CSLI and GPS. The government even got a warrant in this case, perhaps recognizing that fact. But if we want to go down that route and talk about *Carpenter*, and there are two points that the government has made for why it

doesn't fit, one that it is voluntarily conveyed to Google, and we are arguing that it is not truly voluntary, that it is not truly shared in this same sense that CSLI is not truly voluntary and shared with the company.

Here the process -- the difference being it is technically possible to turn on and off location history; however, that process of turning it on and off was highly deceptive and at the very least not meaningful or informed. But even if the Court doesn't want to go down that route, mapping and navigation apps are an essential feature of modern smartphones.

This was something that the Supreme Court recognized in *Riley* and in *Carpenter*, but when explaining the importance of cell phones to people in daily life, the Court recognized explicitly that mapping and navigation services are a part of that. And it's difficult to imagine a modern smartphone that would not provide those types of services.

Here, I think, because of the way that Google set up their opt-in process for location history, because of the way that they warned users against turning it off, saying their functionality of their phone would be degraded, that things would no longer work if they turned it off, there is a suggestion here

that this was essential to those basic features of the phone. And it would not have been apparent to users that they could turn it off and still use maps or still use Google Assistant because Google didn't tell them that. In fact, it told them the opposite. If you turn this off, bad things are going to happen to your phone.

So a reasonable user, looking at this, may not understand what they're turning on. And Google may warn them, and does warn them, against turning it off, saying that a basic function of their phone is going to be degraded if they do that. So, in that sense, we would argue that, as in *Carpenter*, this information was not voluntarily provided.

THE COURT: So, Mr. Price, I don't want to ask this question in a confusing manner, but I probably will. So, I think, for instance, this argument, you are suggesting that Google is essentially burying information about how to turn off location history and suggesting that turning off location history is problematic to the working of the phone, and at the same time you're saying only a third of folks have it turned on. So aren't those propositions contradictory?

MR. PRICE: Well, I think the ease of turning

it on might explain some of the volume there. But it's not necessary at the end of the day to find that. I think even if some -- there are going to be people in this world who actively want location history on their phone. Perhaps Mr. McGriff wants it on his phone.

I do not believe that doing so means that he has no expectation of privacy in that data, that only people that get duped into turning it on have an expectation of privacy. I think, as Google explains, this is user content. This is user property in the same way that email and photos stored with Google are user property and user content. And, therefore, searching any bit of that, even a little bit, is a search.

Google likens it to keeping a travel diary. So if you are interested in this feature, and you turn it on, Google says, Well, we're storing it in your account. Just like you might create a map with pushpins of where you've been, here's a digital equivalent that you can go back, and you can look at, and it's in your account, and it's accessible in the same way as your email, as your photos. And they treat it the same way. They treat it as user content. According to Google, it's not a business record.

What business record -- companies do not generally let customers delete their business records, yet that is something that Google permits with location history here. You can edit your location history.

THE COURT: Right. So I understand those points. So my question was the dissonance between saying both that it is not voluntary to give it over because it's so hard to turn off placed next to the fact that two-thirds of folks don't have it on, which, presumably, means they've turned it off.

MR. PRICE: Certainly some people are not enabling location history. Some people may not have occasion to or need to enable Google Assistant or may be wise at this juncture to what location history is.

I think either way you look at it, under sort of expectations of privacy test under *Carpenter* or as user data, user content that is their property, it's a search. So what I'm saying is there are two ways of getting there. And it's not necessary to find that somebody got duped in order to reach the conclusion that the Fourth Amendment protects this information.

THE COURT: Okay.

MR. PRICE: The idea that -- the other argument the government advances is that *Carpenter*

shouldn't apply because the length of time here was shorter than the seven days that the Court was talking about in *Carpenter*. I want to address that briefly, first by noting that the reason the Supreme Court chose seven days was not because it's a magic number. It was the shortest amount of time of all of the court orders for location history. So the shortest one was for seven days. That's the one the Court considered. And it is worth noting that in response to that court order, the government only actually received two days' worth of location information.

But the Court was clearly recognizing that CSLI requires some stitching together in order to paint this mosaic, to paint a picture of somebody's daily life, because any one location point from Southside location information is going to give only a fairly rough estimate of where somebody is.

The Supreme Court talks about putting somebody inside of a pie wedge that's, you know, a couple miles wide. And we would say that CSLI, at least a little bit of it, is probably enough to identify somebody's neighborhood or the ZIP code that they're in, but it is not going to be sufficient to say which house they were in.

And so the Court was looking for a way to

say, Well, how much of this do we need before it becomes a problem, before you can figure out where somebody was and what they were doing? And that's how we end up with seven days.

But the test, what they're fixated on, is what that information reveals. How much of that information do we need to get to the privacies of life? And our argument here is that geofence data is far more potent than CSLI.

Even a little bit of Google's location history data is going to be sufficient to identify somebody inside of their home or a church or another business nearby, and you don't need as much data to get the same sort of information.

I would also add that because of the precision involved here, because it does rely on GPS, and it does pinpoint people inside of their homes, as we demonstrated to the Court, that there's an additional consideration here that wasn't present in *Carpenter*, which is monitoring people inside of constitutionally-protected spaces.

The Supreme Court has been clear on this a number of times. The best examples are *Kyllo* and *Karo*, K-Y-L-L-O and K-A-R-O. In *Kyllo*, the Court looked at the use of new technology, the thermal

imager. Even though it was only trained on a house for a few moments, a couple minutes at most, law enforcement was able to determine what was happening inside that house, whether there were people inside that house. And that was enough for the Court to say it's a search. There is something special about homes under the Fourth Amendment. They are the first among equals, so to speak.

And using technology to pierce those walls and see what's going on inside and learn information you wouldn't otherwise be able to learn is a search, even if you do it for a little bit of time.

Karo was the same sort of case with an electronic beeper that had been hidden inside of a drum of chemicals inside the back of a car. That car was driven onto private property. And then the government was able to tell when that drum of chemicals was moved.

And that was, once again, information that the government would have been unable to know otherwise because it was occurring within a constitutionally-protected area that they didn't have a warrant to go and search. And the Court said you can't achieve by other means what you wouldn't be able to otherwise do, that the use of technology doesn't

give you a free pass. It, in fact, invites more scrutiny. And that's been the lesson ever sense, especially with *Jones* and *Riley* and *Carpenter*.

So I would also say that the government had to know it would get this information through either the effective range of Step 1, or, clearly, in Step 2 when people are going about their business and coming home, or going to home, and then we see that dot just sitting right on top of their house.

That was something that should have been obvious to anyone asking for this sort of warrant that even if it didn't get constitutionally-protected spaces in Stage 1, it was certainly going to get them in Stage 2. But, once again, even in Stage 1, the geofence encompasses the entirety of a church in addition to the bank. And so I don't think it's for nothing that the vast majority of data points attributed to Mr. Chatrie, all but two, from location history put him either inside the church or right next to it in a car.

And so the idea that this can't reveal information about people in constitutionally-protected spaces is false. And it should have been obvious that that was what was going to go happen to anyone who was seeking such a warrant.

THE COURT: So are you asserting at all that any of the data turned over placed Mr. Chatrie in his house?

MR. PRICE: No. We're not asserting that the data here placed Mr. Chatrie in his house, no.

THE COURT: Okay.

MR. PRICE: The government argues that this is just like the search of one place. That they name Google. They said they put down Google's corporate address, that that's one place, and it's just like searching one place. They get to search everywhere in that one place.

I think that's a sleight of hand. It ignores the mechanics of the search here. This was not like searching one house. This was like searching 10 million houses, or safe deposit boxes may be even a better example. If you want to look at what this might be like in the physical world, it would be like going to a bank and asking the bank, saying, We're looking for a weapon. We think it's in one of your safe deposit boxes. We would like you to open up every single safe deposit box in the country and look for this weapon.

That is the equivalent of what happened here. It wasn't a search of one place. It was a search of

10 million places or numerous tens of millions of places. And to try and say that this was just a search of one place at Google's headquarters is to ignore the nature of this data, to ignore that it belongs to numerous tens of millions of individuals and not to Google.

Lastly, Your Honor, I'd like to discuss good faith briefly, unless you have additional questions.

So we argue that *Leon* should not apply. That three, at least, of the exceptions that *Leon* specifically identifies apply in this case. And all three exceptions relate back to the probable cause and particularity problems that we've discussed so far, that the judge in this case, the magistrate in this case, acted -- abandoned his judicial role, acted as a rubber stamp. Looked at this warrant for 15 -- 30 minutes behind closed doors. Didn't ask a single question before signing off on it. Didn't care to ask how many people might be searched or how the government would handle the selection process in Stages 2 and 3.

This was a warrant that doesn't look like any other warrants yet the judge asked no questions. This was a warrant that explicitly gave the government the authority to decide who to search and did not ask any

questions.

These are basic questions about probable cause and particularity. But instead of addressing them as magistrate judges in Illinois and Kansas did, the judge here simply signed off and left everything up to Google and the government to work out.

The warrant was so lacking in probable cause, so overbroad, that no officer could reasonably rely on it. There wasn't probable cause to search one person's Google account. There certainly wasn't probable cause to search 19, and there was not probable cause to search tens of millions. Even if the government didn't understand that it was going to search numerous tens of millions of people, it certainly would have understood that the search they had in their mind was still going to bring in a vast majority of people who were not involved in the crime at all, for whom they had no probable cause to search and would not have been able to get a warrant to search under other circumstances.

It was only because of this fig leaf of a three-step process that made it seem like this is something that's okay. Looking at it, it is plainly -- plainly they had no suspects. They did not have probable cause to search Mr. Chatrie's account or

anyone else's. This was a fishing expedition. That should have been known to anybody looking at this warrant.

Likewise, it was so obviously deficient in particularity that it also fails under *Leon*. Giving this sort of discretion to law enforcement alone is what the particularity requirement was designed to prevent, to make sure that every petty officer didn't have the authority to go rummaging through everyone else's private papers, yet that is exactly what happened here.

No, it would not be objectively reasonable to believe that officers would have unbridled discretion to search through the location history of millions of people, especially when they didn't have any suspects.

So, Your Honor --

THE COURT: Well, let me ask you this because a not insignificant amount of your briefing suggests that this task force officer really didn't know what he was doing, didn't know that what he was asking for asked for more specific information when he got a group of 19 in the first instance, and that he should have known it was his requirement to narrow it down. So I'm trying to figure out how that feeds in to what you're saying about the discretion should not go to

the government when it appears that you're saying it's Google who's doing all this, or at least most of it, the thought processing and the narrowing down. Is that entirely dependent on your argument that Google is an agent of the government so they functionally are the government even if this task force officer really didn't understand how the process worked?

MR. PRICE: Right. So I think it's significant that the government and Google had worked out some of these details ahead of time. Even if Officer Hylton didn't know all of them personally, this was a go by.

THE COURT: When you say "Google," you're talking about the corporate level interaction with the Department of Justice? Is that what you mean?

MR. PRICE: Well, initially, it was developed between CCIPS and Google's legal team, and then here we had specific back and forth with respect to this warrant as well.

So, yes, we're saying that Google was functionally acting at the government's discretion here, that Google was compelled to act as a result of that warrant. Google was attempting to follow that warrant. That's what they were saying in response to Detective Hylton when he asked for all 19 at Stage 2

twice. And Google said, Well, we're complying with this warrant that we're legally obligated to follow, and you're not following the process.

So I think it reiterates that Google is acting in a manner that is compelled by law, that they are trying to, at least, follow the letter of that warrant, even if the government wasn't. But that, more generally, the questions that Detective Hylton maybe had about this process are attributable to the fact that this is not a normal process. This is not something they receive training on. This is not something that there are policies about. This is not something that is normally done. And so one would expect, then, there to be some confusion and questions about how it is executed.

This is a reverse warrant. This is not something like Detective Hylton or others would have normally seen or used when you're obtaining information about an individual, an individual account with a warrant that identifies that account. That is the way that this normally happens.

THE COURT: Doesn't this record show that he had done three geofence warrants before? Am I wrong about that?

MR. PRICE: I don't believe it was three

before, but --

THE COURT: I thought it was one federal and two state.

MR. PRICE: I thought it was at least one, maybe two.

THE COURT: So anyhow, he's done it before. So it's not normal, but it's not new either, right?

MR. PRICE: I suppose that is fair. It's fairly new. Even if this is only the second or third time. This is only the first time that we've actually had an opportunity to discuss this stuff in front of a judge. So all of the decisions prior to this, as Your Honor knows, were done *ex parte* based solely on the records available from this case at the time and whatever the government submitted. We still don't actually have copies of the warrants in any of those cases. They're all still under seal.

THE COURT: I just want to ask sort of random questions to make sure I don't forget them.

The United States argues that as far as the opt-in process, that this court should be bound by the testimony of Mr. McGriff because he was able to testify to the specific time frame under which Mr. Chatrie would have been using his phone, and so that your expert, who spoke about different opt-in trees,

consent flows, that I should disregard those. Are you in agreement with that?

MR. PRICE: No, Your Honor. I think Mr. McGriff was able to identify the date and time at which location history was enabled, which is only information that Google has, but Mr. McGriff was not able to say explicitly which consent flow or how it would have appeared to somebody like Mr. Chatrie. And we put forth both of those possibilities. At the time there was the "saves a private map" language and the "saves where you go with your device" language, which happened -- the change happened close in time to when location history was enabled. Mr. McGriff was unable to say exactly which one because he didn't know the operating system and software -- sorry. The operating system version that was running on Mr. Chatrie's phone.

So I think the implication there is that there's some sort of rollout process, and that it doesn't all happen literally at once like flipping a switch.

So, I guess, taking a step back from that, what I would say is that either of those two consent flows take you to the same place. That neither of them describe location history in a sufficient way to

give users informed consent over what they were agreeing to. In both instances it was less than a sentence worth of text that somebody was required to look at. And in the case of Google's Assistant, it was bundled with two other choices about enabling Voice & Audio Activity as well as device information, both of which would have been necessary to run Google Assistant, according to Google.

So, in either instance, whether you want to go with "saves a private map" or "saves where you go with this device," we do not believe that that would be sufficient to give informed consent. And we do believe that the testimony that Mr. McInvaille provided to the Court and the research that he provided or he was able to present to the Court, which the government did not contradict and Google did not contradict, I think both Google and the government were asked if they had any information to contradict Mr. McInvaille's testimony, and they said no to both.

THE COURT: All right. So, you mention a couple of times, perhaps more than that, both in argument and in briefing, that through the steps that this warrant proceeded from, Step 1 to 2, to Step 2 to 3 with no supervision, is it the case that by requiring an officer, an executing officer or law

enforcement officer, to have each return at Step 1 reviewed, and then before you go on to Step 2 or at Step 2, would that solve the constitutional concerns?

MR. PRICE: I think it might alleviate one concern with particularity. What it does not address is the Step 1 confusion, let's put it that way, about what is to be searched and seized in the first instance, which database is going to be searched, what are you counting, what area are you actually searching. All of those at Stage 1 were still left up to Google and the government to decide.

So Stage 2 and Stage 3 is more obvious because it explicitly leaves that decision up to the government. But Stage 1 is just as deficient in particularity. Even if it doesn't explicitly leave that decision up to Google and the government, it effectively did.

THE COURT: So I want to confirm, you say that the government and Google had agreed to certain parameters, for instance, searching Sensorvault. Is it the case that my record shows that the government agreed to that or that Google just did that knowing that the other repositories wouldn't have responsive information?

MR. PRICE: So I don't think we have as much

visibility as we would like into the origins of these warrants with CCIPS and Google discussing, but I don't think that ultimately matters to the outcome here.

THE COURT: So that's what I was trying to get to before. When you're saying that there's a discussion between Google and the government about what is going to be searched, i.e., Sensorvault, you're not saying that Task Force Officer Hylton had that discussion with anybody at Google. You're saying Google legal office had that conversation with CCIPS.

MR. PRICE: It appears that that's what happened. What I am saying at the end of the day is that a judge didn't say it one way or the other, which is what's required. I don't know who suggested what first, but the information was never presented in the warrant or application. It never mentions location history once, and that's a fundamental decision about what gets searched that should have been up to a judge and not some combination of Google and the government.

THE COURT: At any level, corporate level --

MR. PRICE: Correct.

THE COURT: -- or with this particular warrant.

So, with respect to the --

MR. PRICE: I was just going to go grab a

note.

THE COURT: You can go ahead. Maybe it addresses some of my questions.

MR. PRICE: First, I wanted to add to Your Honor's question about which consent flow would have been operative at the time. Mr. McGriff on pages 295 to 297 of the transcript acknowledges that he was uncertain of what language was baked in at that point in time into the phone. So that's the source of the uncertainty as to which particular language was or would have been seen.

And as we've mentioned, either way it shouldn't effect the outcome, I think, too, too much. The consent flow issue is also interesting here because we talked about what happens when you attempt to turn it off, and those sort of warnings that you get. However -- and this speaks to the voluntariness point as well -- merely turning it off does not delete the stored information that Google may have. So even if I turned off my location history right now, if I didn't actively then go and delete everything, the search would still run against me as everyone else.

Similarly, even if you delete that information, it doesn't actually turn off location history. So enabling or when Google enabled an auto

delete feature long after the facts of this case, you might be mistaken for thinking that that would have some effect on the collection of location history. In fact, it does not. And it further adds to the confusion here.

And lastly, we'd say that the consent flow isn't as probative of the expectations of privacy as the way that Google treats that data. So Google considers location history to be user content. It stores it as user content in user accounts. That's why their system is indexed this way because it belongs to the users. It is not Google's business record. And whatever weight the Court wants to put on that consent flow, it doesn't change the fact that that is individual data, the modern equivalent of their private papers stored in an individualized account.

THE COURT: All right. So my first question is, with respect to good faith, if Task Force Officer Hylton had gotten even one geofence warrant before and there is even one case that says that it's permissible, why doesn't that satisfy good faith?

MR. PRICE: There was no case saying it was permissible at the time. All of these Illinois cases came after this case. In fact, they were using some

of the early record in this case to base their decisions on. So there was no court decision on this.

In fact, I would say the -- if anything, however, the Supreme Court's focus on probable cause and particularity for the last few hundred years would signal to a reasonably well-trained officer that they need both probable cause supporting their warrant and that it must be particularized. Both of those things were glaringly absent here and that should have been apparent on its face to both Detective Hylton and to the magistrate who signed it. And the fact that Detective Hylton had done this once or twice before, I don't think changes that whatsoever. Especially, if there was no pushback or --

THE COURT: We don't know, right? All we know is that he had at least one approved, right?

MR. PRICE: We know, Your Honor, that Google, at least, reports having received quite a few of these. And it is interesting to note that this is the first case where it's actually being tested in court. Part of the reason that happens is because the geofence warrants are not always successful in identifying a suspect.

There was a different arson case being investigated in North Carolina where the geofence

warrant was reported in the news but failed to actually identify a suspect. And that could have been for any number of reasons, but one good one would be he was one of those two-thirds that did not have location history enabled.

There's a large number of these warrants that do not produce results. It is a fishing expedition. You're not always going to get a fish every time.

THE COURT: So what of the cases that we now have do you think I should look to most closely when reviewing your position?

MR. PRICE: I'm sorry? Which --

THE COURT: Which of the reported or unreported but available geofence cases that we now have is the one or two that you think I should look to most closely when reviewing this case?

MR. PRICE: I think Judge Weisman's opinion and Judge Fuentes's opinion are both very informative and well reasoned based on the facts that were available to them. I would say none of these opinions attempt to grapple with the scope of the search at Stage 1, which, simply, I don't believe was apparent at the time. But of the four that are out there now, certainly Judge Weisman and Judge Fuentes have very strong reasoned opinions when it comes to probable

cause and particularity.

THE COURT: All right.

MR. PRICE: Thank you very much, Your Honor.

THE COURT: I think those are my questions for now.

MR. PRICE: Okay. Thank you very much.

THE COURT: Okay. Thank you.

All right. So I think this is a good time to take a brief break. And we'll be back in 15 minutes, which takes us to 11:40. All right? And we'll begin with the government's position. We'll take a recess.

(Recess taken from 11:25 a.m. to 11:40 a.m.)

THE COURT: All right. I'll hear from the government.

MR. JUDISH: Thank you, Your Honor. Nathan Judish on behalf of the United States.

As we've argued consistently in this matter, there are three separate and independent reasons why this court should deny the defendant's motion to suppress.

First, that the defendant had no reasonable expectation of privacy in any of the information the government obtained from Google.

Second, that the government obtained it pursuant to a valid warrant.

And third, that investigators relied on the warrant in good faith.

I think the logical way to talk through this is to start with the question of a reasonable expectation of privacy. So I will begin with that.

I think that whether someone has a reasonable expectation of privacy turns in large part on the nature of the disclosure. And the Supreme Court has repeatedly held that one retains no reasonable expectation of privacy in information voluntarily disclosed to a third party.

And so I think it's really important to take a close look at the notion of the services Google provided here. And, essentially, Google's function here is as a location-based service provider. And so the real question is, what does a user of location-based services disclose to a location-based service provider in order to obtain location-based services? And I think the answer is pretty clear. The user discloses location information.

So consider what Google actually -- the services they -- the nature of the services they actually provide to the defendant. The main service that you disclose your location for is to get recommendations with your commute; driving

instructions and such.

So what does that mean? This isn't -- this isn't a case of someone just having Google store their location in order to create a map, although that may be one thing that they do, but you also disclose your location so Google, as a service provider, can help you get from one place to another quickly. And that involves not only Google knowing where you are and where you're going, but also Google knows where everyone else is going at the same time as well. So what you have, generally, is vast numbers of people disclosing their location to Google from which Google can assess where they are and how fast they're going and from which Google can spot traffic problems and tie-ups, one way or another, and then Google sends out advice.

You know, I'm driving down here last night on I-95 and Google says there's an accident up ahead. You can save 21 minutes by taking another route. Google doesn't know that just from my location. Google knows that from the location information it's getting from everyone.

So what we see here is that Google is using everybody's location to essentially provide useful advice to everyone. This is not people keeping their

location secret or private or anything like this. This is a big communal effort to pool location information in a way which lets Google then provide generally beneficial advice to everyone. And so it's just not kept to yourself.

And it's true that Google doesn't normally disclose any particular individual's advice [sic] to others in giving out that advice, but it's clear from controlling Supreme Court precedent in the *Miller* case that that doesn't matter. The point is, users disclose their information over to Google, and then Google, you know, is free to use that information and act on it, and so on.

THE COURT: Well, I do think you have to address the fact that, you know, *Miller*, and what we're discussing here, are facts of a different order. Right? So it is not the case, or I guess I should ask you, do you think that folks are knowingly or willingly giving over information about their location that Google updates every two minutes? I just don't think you can say that.

Most folks don't know, I think, that Google is keeping this on a two-minute loop.

MR. JUDISH: Well, as an initial matter, you can deduce just from the driving services that they're

looking at your location pretty much directly. I mean, it is really like there's something going on right now, and they act on it right now. Google has to know your information right now and act on it.

And beyond that, I mean, Google says, and it's also clear that we know from the *Smith v. Maryland* case that it doesn't matter whether you know or not that they're going to store information. The fact that you disclose it is sufficient.

So in *Smith*, you know, there was an argument that, well, customers didn't know that the phone company would actually keep records of that information, and there it didn't matter.

But, you know, as far as the -- and in addition to sort of being able to tell from using the service --

THE COURT: So I'm going to stop you there. Are you saying there is no aspect of the facts in either *Smith* or *Miller* or our case that differentiates them? The numbers we're dealing with here, if they are exponentially more than those in the other cases, that it doesn't matter?

MR. JUDISH: I mean, I don't think the frequency of storage makes much difference. I mean, you can store -- I would say, one, are users aware of

it? Well, they certainly can be because unlike with the phone company where you can't really see all the information the phone company has traditionally stored about you, your records are available to you at Google. You can log on, look at your account. You can go and see everything that they have stored. So, that's, I mean --

THE COURT: So, I'm going to say, sir, you are speaking really quickly. And I can see that my reporter is trying to keep up with you, but I can hear everything you're saying. We just have to be sure that the record follows, too.

MR. JUDISH: I will try to slow down, Your Honor.

THE COURT: Okay. Thank you.

MR. JUDISH: So, anyway, with Google you can see everything that you see stored. And so, you know, users can be aware of exactly what there is.

And, in addition, once you agree to Google saying "saves where you go with your devices," I think the frequency of it just doesn't make that much difference after that.

I mean, you can store whether it's -- you know, because people move quickly. In order for that to work well, they have to store relatively often.

And just a small, you know, small intervals, I think just don't have a great deal of significance.

So, another, I think, noteworthy aspect of how Google uses the information is in their advertising and the radius targeting that they do.

So Google, from location history, they make -- to begin with, they make certain inferences about your interests, and they target useful advertisements to you based on that. Again, that's more than just a storage service, but it goes beyond that. The radius targeting part is they will sell to customers or to advertisers the ability to place advertisements to people within a certain radius. And then in order to measure the effectiveness of that, they will subsequently examine location history information of users to see whether they have actually visited the particular store that was doing the advertising.

So that's -- I mean, that's really essentially the equivalent to a geofence because it's around the particular store that has done the advertising. So Google is doing with its own data that users provide to it, and they're quite up front about this, something which is remarkably similar to geofencing, you know, a geofence around the individual

advertiser's stores in order to, you know, provide this store visit conversion statistic to the users.

THE COURT: Yeah, but they don't identify -- I mean, they explicitly don't tell the advertisers who they are identifying.

MR. JUDISH: They don't.

THE COURT: So it's not generally the same.

MR. JUDISH: Well, again, the equivalent for the purpose of showing that the information is disclosed to Google, and it's really not necessary for the third-party doctrine for Google to, then, normally in the ordinary course of business disclose it to others. Just like a bank doesn't normally disclose your expenses to third parties outside the bank, but what you look at is what is disclosed to the party from whom the government got information.

And I think it's clear from that advertising function that you are disclosing your location information to Google.

And then that's just -- this so far has just been analyzing the nature of the service Google provides. It's also worth looking more carefully at the opt-in process and what it takes.

And as Mr. McGriff pointed out in his testimony and affidavits, it really takes a

multiple-step process before Google knows -- will ultimately store someone's location history.

So you start off with a cell phone. It's just a little electronic device sitting there. It doesn't know its location unless you first turn on the feature for your cell phone to get it to determine its location. So that's the first step you have to take.

Now the phone knows its location, but it's not telling anyone because you haven't told it to share that information with anyone. So the next step you have to take is you have to tell it to -- adjust your phone so it will share that information with apps so apps can provide you location-based services. So you do that and now the information may be shared with a Google app.

Well, okay. Google -- that's fine. Google may be able to use that location information, but it still doesn't know who you are because you haven't signed on to the Google app on your device. So that's another step you have to take before Google will end up with location information.

Okay. So you sign in on your device and now Google can determine your location.

THE COURT: Slow down.

MR. JUDISH: Slow down. This is still too

fast? All right.

So now Google can determine your location information. And it still won't store that information unless you take the additional step of opting in to location history. So all those things are affirmative steps you have to make before Google will store your location history.

And so then I want to address, because we have it in such detail, the actual opt-in process for location history. And here I think it's important -- I just want to say a bit about the record.

So, McGriff testified first through a sworn affidavit, and then he affirmed with his testimony that he stuck by his affidavits. This is from Government's Exhibit 3C at paragraph 7. Under the supported consent flow as of July 9, 2018, across all applications and services and across all Android devices and operating systems a user who opted in to LH, location history, either directly from within device settings or when attempting to use a feature powered by LH, such as features within the Google Maps application.

THE COURT: So when you read, you're even faster, which is what every human being does.

MR. JUDISH: Would be presented with an

opt-in screen containing the following text.

So McGriff said, you know, this was across all devices, across all operating systems. This was necessary opt-in language. And what he said also in his testimony was that this consent copy has been static. That's on page 271 of the transcript. He said there was possible additional descriptive copy which could change, and that, the descriptive text, he personally could not be sure about, but the actual -- this actual consent copy, he said, was static and was essential in order to opt-in. So that's why I think this court can look at the -- this consent opt-in he presented in his affidavits and be sure that that is, in fact, what he would have seen when he -- what the defendant would have seen when he opted in. And what that says is "saves where you go with your devices" and "this data may be saved and used in any Google service you are signed in to give you more personalized experiences. You can see your data, delete it, and change your settings at account.google.com."

So, I think this text really gives the core of what you're agreeing to. It says that Google's going to save where you go with your devices, and it says that Google can use that is information to

provide you with services. And that's what happens with Google's location-based services. And to that you're given a choice, either "no thanks" or "turn on," and we know because the defendant opted in on July 9, 2018, that he did, in fact, say to turn it on.

All right. So, I think all of this shows that the defendant did, in fact, voluntarily disclose his information. What does the law say here? Well, the principle that -- over and over in every single case, the Supreme Court that has addressed it, it's held that one retains no reasonable expectation of privacy in information voluntarily disclosed to third parties.

To be clear, this is not just about business records. The defendant keeps characterizing -- they're saying, well, these are not business records. I don't think it -- I mean, I think Google is clearly using the records for a business purpose, but the third party doctrine does not depend on whether or not something is a business record. It applies to conversations you do in the presence of others, for example. We know that from the *Hoffa* case.

The Supreme Court has affirmed it in multiple other contexts. We have it for everything you give to an accountant. That's the *Couch* case. We have it for

telephone dialed number information in *Smith v. Maryland*. We have it for bank records in *Miller*. And the Supreme Court has never, ever rejected that principle.

Now, *Carpenter*, the Supreme Court, obviously, did not find it applied, but the key point about *Carpenter* is that the reason it didn't apply is that the Supreme Court found that the cell-site records were not voluntarily disclosed to the phone company. And it did that for three reasons. And if you look at those three reasons, none of them apply to the location history or location information disclosed to a provider of location-based services.

First, the cell-site records are collected automatically if you just power up the device. No other affirmative action is necessary. So if you want to make phone calls, send texts, you get a cell phone. It just happens behind the scenes automatically, and there is no special opt-in process. There's certainly nothing that looks like what we have here.

The Supreme Court also noted the impossibility of deleting your cell-site records, whereas here, not only, you know, you can delete your location history stored by Google any time you want. And it's -- significantly, this fact is emphasized

over and over again by Google, even in its very minimal consent, you know, short brief text in the opt-in process. It highlights the fact you can review and delete your information at account.google.com. If you look at the Google privacy policy, it further has a long section explaining all the different ways you can delete your Google data. You know, individual data, service by service data, getting rid of your account, all that is explained at length in the Google privacy policy. So, that is not at all like cell-site records.

And, finally, the Supreme Court noted that having a cell phone was indispensable for participation in modern society. Well, I think it's quite clear that that's not the case of Google location history. Obviously, one way to establish that is empirically. We know now that only about a third of Google customers have their location history enabled. And the second way you can establish that it's not essential to participation in modern society is looking at the features associated with Google location history. They're okay. They're helpful in some circumstances, but they're just not that big a deal. The tips on your commute, finding your phone, you know, useful advertising all may be nice to some

customers, but they're not indispensable to participation in modern society.

THE COURT: Well, to be fair, you should address why Mr. Chatrie is turning to that argument. It's because Google requires a warrant under the Stored Communications Act. And so they're saying that's an indication that Google is calling it a business record. Right? Isn't that what they're saying?

MR. JUDISH: They're saying Google says it's not a business record, but I don't think whether it's a business record or not has bearing on whether it's indispensable for participation in modern society. So --

THE COURT: Yeah, but they're not arguing -- they're arguing under the Stored Communications Act that it's content. Right? That's what they are arguing.

MR. JUDISH: That's what Google is arguing. So I think whether something is classified as content under the Stored Communications Act is not that important here. It affects the rules, the statutory rules, for what kind of process the government can use to get information, but I think as a Fourth Amendment matter, it's not critical. The question is whether

Google has -- whether the records are voluntarily disclosed to Google or not.

So, and the same thing, the conversations in *Hoffa* were certainly content. That's people speaking. But because it was voluntarily disclosed to the persons who heard them, it didn't affect the -- the Fourth Amendment was not impacted when the hearer disclosed that information to the government.

So the -- whether its content has some, you know, legal significance on the kind of process you get. So I recently saw that Google had objected to a proposed state law in Texas that would allow warrants to get prospective location information from Google. They say because it's content, actually the federal law requires a wire tap order. I mean, all this is complicated statutory stuff, but not really implicated in this case. This case is about the Constitution and the Fourth Amendment, not statutory definitions or statutory rules.

I would note another point -- well, I guess, on just -- it's worth saying a little bit about *Carpenter*. *Carpenter* is, as the Supreme Court emphasized, you know, a narrow case. It's about protecting long-term comprehensive location information. The Supreme Court was clear that it said

a warrant would be required for seven days or more.

The defense here is citing *Carpenter*, essentially, for the notion that anything -- private or sensitive information requires a warrant. That is not *Carpenter*. That's not what *Carpenter* held, nor is it what any court subsequently has decided. I think, you know, *Carpenter* is no longer a totally new case. This week is its third anniversary a couple of days ago. I'm not aware of any courts who have interpreted it so broadly.

Instead, it's a uniformly -- courts have taken the Court, you know, at its word and treated it as a narrow opinion designed to protect comprehensive, long-term location information.

THE COURT: So address what they just argued. Right? They said, yes, that nobody has broadened it because we're the first folks that now know exactly what Google is doing, and we know how in depth it is, and that it covers, even if it's only a third of users, it's tens of millions. And if a court had known that, they might have come out differently.

Just agree, first of all, that other courts did not have that information.

MR. JUDISH: So, I don't think other courts had that information, other courts who have ruled thus

far. So, I think, I mean, that's very different than the *Carpenter* issue because, first, *Carpenter* is, you know -- we aren't obtaining comprehensive, long-term information about all those other people. In fact, I think it's quite doubtful that there is any Fourth Amendment significance at all for anyone whose information we did not return or who was not returned for other than the 19 people. I mean, I don't think it's a search with respect to the 19.

THE COURT: Wait. You're going way too fast. I didn't hear the last sentence at all.

MR. JUDISH: So leaving aside the 19 people, just talking about all of the others, I don't think that there's any Fourth Amendment significance at all to a provider the way a provider like Google uses automated processes to find very narrow specific information in a large database. You know, I don't think there's any significance for people whose information is not returned to the government. So --

THE COURT: Wait. Wait. I'm going to ask a question about that.

So with respect to how Google does the search, first of all, they are saying that Google is a government agent. Do you agree with that? Under the law, that they are treated as an agent.

MR. JUDISH: I don't think it's clear. When you're talking about compulsory process -- and from Google's point of view, this works an awful lot like a subpoena. And I'm not sure that someone responding, complying with compulsory process of one sort, is really quite the same as other kinds of agency relationships.

So I don't think -- I wouldn't concede that it's an agency relationship. I think things are different in terms of compulsory process. You know, when you're in litigation, and the other side receives a subpoena, are they really your agent when they're complying with a subpoena? I don't think it's clear on that. I don't think there are cases -- I'm not aware of cases that specifically address that.

THE COURT: Right. Okay. So they're saying you're not aware of it because we're the first folks that know that when the government says we want to do a geofence for this particular period of time, now we know that it's functionally Google who says, Okay, we're going to look at this area, and we're going to do it in this time frame, and it's our algorithm about how it works, and you don't get to know the algorithm. Right?

So, if you get a subpoena, it is not the

case -- well, maybe there are cases, but it's not the case that a business can say to you "I'm not going to tell you how I search for documents," right?

MR. JUDISH: Well, I mean, Google is telling -- Google's quite clear now about how they respond to the process. I mean, we give them the coordinates, and they look at each data point in their system, and they decide whether it falls within the range or not.

I mean, the part that Google is more secretive about is how they calculate the people's location in the first instance. I mean, that's the part which -- you know, so how did they come up with the particular numbers in their system for all those data things. But once they get -- they work here quite clearly, everything they did, once they got the warrant from us.

THE COURT: Well, that may be a little bit too simplistic because they said there is a range. They said that they found a range. They said there's a probabilistic return rate, like 68 percent they found appropriate for advertising, right? So I have to say, useful advertising is more a Google term than it might be a user term, but, anyhow, it's advertising. They target advertising.

So it is -- they're not saying that in a way that the government can test that it's reliable. Right? So this is what Mr. Price was just saying. He was just saying, Yeah, we don't know about the ones that haven't made hits or why because they haven't made hits.

So why is the government allowed to just say, Google, we think you're doing it right, and we'll use it when it hits? Isn't that something the government should have some input in? It's different than a subpoena.

MR. JUDISH: All of that stuff happened prior to the government getting the process in this case. Google has its own internal algorithms which they use to estimate where its users are.

THE COURT: I know, but you get the warrant knowing they have this system you don't understand, correct?

MR. JUDISH: Well, I mean, we've looked at the data that they produce, and we've seen that it's pretty accurately what --

THE COURT: It's 68 percent. Or are you saying it's better than 68 percent?

MR. JUDISH: I'm saying that it seems consistent with the notion that 68 percent of the time

the user falls within the display radius at the point that Google estimates that they are. And I believe we had testimony saying that the rest of the time it's not like it's super far off. It's often near the outside bounds of that, of the circle that Google has.

So it's not like it could be, you know, you think it's in Richmond, and you're right 68 percent of the time it's near the bank, and the other time it's, you know, across town or in another state or something like that. That's not the way it works at all.

And so what you have here, essentially, is information which is, you know, like all information, you know, it has some uncertainty in it, but it goes to -- it would ultimately go to the weight given the evidence, not the admissibility, because we've observed the information and it seems to be -- work the way Google describes it. That it --

THE COURT: Do I have any evidence about how often the geofence fails? Like how often there's just a zero hit?

MR. JUDISH: You mean, like we get a geofence and it ultimately proves unsuccessful in locating anyone or any evidence? I don't think there's anything in the record about that, Your Honor.

THE COURT: So here's the commonsensical

layperson's perspective. And so I'm really trying to give you an opportunity to explain it away. If there were drug testing that were 68 percent reliable, would it be admitted?

MR. JUDISH: I mean, I think -- I mean, I don't know about the context of drug testing, but, I mean, I think it's, you know, the definition of evidence is fairly broad. And so I would say it's evidence, but it's not all that reliable evidence, and you would hope there would be more reliable evidence.

And so, you know, in a case like this, if we go to trial, you would certainly want more than just the geofence information, and yet it's still evidence that the government collects, and then it helps direct their further investigation, which, if things go well, comes up with evidence which is even stronger and better and more probative of guilt or innocence. But it's clear that this meets the standards of what is evidence because, you know, it is helpful information which helps prove the facts which are at issue in the case.

THE COURT: Okay.

MR. JUDISH: So, a bit more -- I wanted to touch a bit more on the law associated with the third-party doctrine.

First, the defense was just -- made a point saying that sometimes you can use this information to place a person in a private space, which they suggest is a problem under *Knotts* and *Karo*, but *Knotts* and *Karo* aren't third-party doctrine cases. *Knotts* and *Karo* involve installing surreptitious transponders and tracing them. In those circumstances, we if get information from a private space without a warrant, that's a problem because it's a search.

Here, however, when we rely on the third-party doctrine, that's not an issue because the leading or a leading third-party doctrine case is the landline telephone case *Smith v. Maryland* where every time someone makes a landline call from their house, we place them in their house. And the Supreme Court says that does not matter. It's still information which is voluntarily disclosed to a third party. That issue is explicitly addressed in *Smith v. Maryland*.

Again, I just note that subsequent to *Carpenter*, the cases have all interpreted it narrowly. Within the last few weeks we had a Seventh Circuit case, *Hammond*, which held that there is no reasonable expectation of privacy in getting like six hours or so of prospective latitude-longitude-GPS-type data from an individual cell phone.

And the Court looks at *Carpenter* and says *Carpenter* is only about long-term location information. And so that *Hammond* case is three times the duration of the information at issue here. And still the Court found that the Fourth Amendment was not violated.

THE COURT: But isn't *Hammond* different in that they had a suspect in mind? What the defense is saying here is that it's a reverse search. It's like we don't know who it is.

MR. JUDISH: *Hammond* was a specific person, but as far as whether one has a reasonable expectation of privacy in the information in the first place, I just don't see -- I don't think it makes a difference. I mean, I think that it would be -- it would be -- you know, those are very different kind of warrants between a warrant for an individual's location and this type of warrant. But as far as whether one has a reasonable expectation of privacy in the information, really, I don't see how that can turn on the particular kind of legal process the government got to obtain it or didn't get to obtain it.

The question of whether there's a reasonable expectation of privacy, I think, is sort of prior to whatever kind of process the government uses to obtain

it.

One final thing on this point, just referring to *Smith* and *Miller* as relics, I mean, you know, most Supreme Court cases don't, like -- they don't, like, age out after a little while. They get reversed by the Supreme Court or they remain binding law. The Supreme Court actually affirmed them in *Carpenter* that they were still -- their continuing validity. So I just don't think you can dismiss continued binding Supreme Court precedent.

THE COURT: They're not talking necessarily about the law. They're talking about the technology involved. I mean, you have to concede this is different technology. The scope is what they're talking about, the breadth, the numbers, the detail. So, you know, in the hearing that I saw, and I think Google suggests, that if you were to go backward, as these folks are, you have -- you can make a map of where you were. You can make a little line of where you were within a period of time. And so two hours.

The question is, if you're voluntarily giving over your information, is the notice that Google is giving putting you on notice that at any two-hour period you can be mapped exactly where you are? That's their point, right? That, sure, if you're

driving down on 95, maybe intellectually you can say, Oh, you know, I have maps on. There's a tractor-trailer crash, and they're going to take me down Route 1 instead. But does that really -- does that really put a user on notice that every two hours of their life Google can track what you're doing in a comparable way? So you're saying yes.

MR. JUDISH: "Saves where you go with your devices" doesn't have qualifications with it. There are no limitations. I mean, I think, you know, that's what they do. That's what they say they'll do, and that's what they do, and that's what they show you they do if you log -- if you go where they direct and look at the data that's stored.

I just don't know. "Saves where you go with your devices" and we really mean it? I mean, I think the defense kind of explored this, and what you end up if you start trying to cover much more than that is the wall of text, which nobody would read.

THE COURT: The what? I'm sorry?

MR. JUDISH: The wall of text was the phrase that Mr. McGriff used when defense counsel suggested a rather lengthy description that they thought that Google should provide. And if they did anything like that, we'd hear, well, nobody reads that. So,

instead, what Google does is they provide a very concise description, "saves where you go with your devices," which captures what it is, and then they have an arrow, an expansion arrow, which goes into more detail, and they have a link where you can go to the website and actually see the data. I just don't -- I don't think you can do more to explain, you know, than that to effectively get across what's happening here. You tell them what you're doing and you let them see the data.

THE COURT: Well, not to mince words, but do you think it would make a difference to a user if it said "updated every two minutes"?

MR. JUDISH: No, I don't. People want the service. And if you don't do it every two minutes, it's not going to be all that effective. It's saving where you go with your device. People move quickly quite frequently and make brief stops in places, and so it wouldn't actually serve its purpose if they did much less.

THE COURT: All right.

MR. JUDISH: So, moving on to the warrant, if you don't have any more questions on the expectation of privacy.

THE COURT: If I do, I'll go back.

MR. JUDISH: All right.

So the magistrate here had a substantial basis for issuing this warrant. And the question here for this court is not would this court issue the warrant exactly like this. It's whether the magistrate had a substantial basis for issuing the warrant. And so, you know, several -- there have been in recent times several magistrate judges, federal magistrate judges, who've issued opinions on this.

They sometimes want more in the way -- they say I want more particularity in this way. This application is too broad. Those do nothing to show that there's a problem here, because, you know, the facts of those cases are different.

In one case, the geofence extends out into a denser urban area. In one case it involves a facility with several layers of apartments above it. And so getting a geofence there is just factually very easily distinguished from here.

So if you -- the question is, first, did the magistrate have a substantial basis for finding probable cause? And the question here is, was there a fair probability that Google had evidence of crime? And the facts set forth in the affidavit were sufficient to establish that.

The affidavit showed that a crime had been committed, that the robber appeared to be using a cell phone, and then established that most people have -- or that most cell phones are smartphones, that all -- nearly all Android and some Apple smartphones will be linked to Google, and that Google can store location information. That established a fair probability that Google would, in fact, have evidence of the crime.

And I think it's important to note here that evidence is not just about identifying the robber, but, you know, one of the purposes of it was to form a fuller geospatial understanding of the -- that's from page 5 -- of the warrant and timeline related to the investigation.

And so I sort of see the geofence warrant in this case as sort of similar in quality to surveillance videos. It gives you a picture of what went on at this armed bank robbery, at the time of it, sort of the people, where they were, where they're coming and going. So it's a way of going and essentially getting a new perspective on a crime scene. And it certainly does that. And so that's good evidence and, you know, a fair probability that there was evidence of a crime.

Again, it can be used to identify

accomplices. You know, it mentioned other potential witnesses, and they may not have been able to spot any other witnesses before they sought the warrant, but there could have been someone sitting in the car there back where the defendant parked. And so the notion that it was too late to -- sorry. I don't mean witness. Accomplice. That it was too late to look for other accomplices. Absolutely not. It was a totally appropriate part of this warrant to look for accomplices. It was -- that's included and is the basis for the warrant and is part of the reason why there was probable cause to get this particular warrant.

All this, the sort of a broad interpretation of what is acceptable for a search warrant, is confirmed by the Supreme Court's decision in *Messerschmit v. Millender* where they talk about sort of the broad -- sort of different reasons you might want to gather evidence, including things like (unintelligible) defenses and stuff.

THE COURT: You are really --

MR. JUDISH: I apologize for that, Your Honor.

THE COURT: I didn't hear what you said.

MR. JUDISH: So, in -- a broad conception of

evidence is confirmed by the Supreme Court's decision in -- I'll just call it *Millender* -- in which they look at a warrant and look at the reasons behind the warrant, and it's things like rebutting possible defenses. So it's a very broad conception of what constitutes evidence under a search warrant.

And this warrant sought this location information not just to identify the robber, but also for these other purposes, which are explicitly mentioned in the affidavit. So the notion of the affidavit being all about finding the robber just isn't true. You know, we don't look to, like, well, it's mostly about this other topic, and, therefore, this thing mentioned in the affidavit doesn't count. That's not the way things work.

THE COURT: So I'm just going to totally change courses so that I can have you address this on this record. And I'm going to tell you right now, I don't think it's an issue, but this is obviously a state warrant from a state magistrate. And so this magistrate was fully impowered to do what he did.

I guess I would want you to say this magistrate, who had, I don't know, a couple years experience, did not have a law degree, right? He had a college degree. And it's a pretty broad warrant.

And so my question is, do you think that the Virginia law should hold under this circumstance, right? I mean, federal magistrate judges have law degrees. And it's not clear to me that the General Assembly, when it was figuring out how magistrates work in the commonwealth of Virginia, were anticipating that they could sign warrants that searched tens of millions of user records. So I just want you to state this on the record.

MR. JUDISH: I think the magistrate was authorized under Virginia law to issue warrants, and the government doesn't always get to pick and choose. I think we have testimony in the record that there was -- the preference of the Virginia courts was to go to the magistrates rather than the state judges. So when judges -- we do what we're told, Your Honor. And this is constitutionally permissible under *Tampa v. Shadwick*, and this was a judge authorized for Virginia to issue warrants.

I still -- I still -- I disagree with the characterization of this being a search of tens of millions of people. I think the government obtained no information about those -- about anyone other than the 19.

The government can't tell, you know, if

you're not among those 19, anything about where you were that day. It doesn't know whether or not you have a Google account. What does the government know about those 19 people? It doesn't know whether you have a Google account or not. It doesn't know whether you activated location history or not. It can't tell anything about those people.

THE COURT: Why don't you distinguish the example he used about, okay, we're going into a bank. We know one of your boxes has a gun, but we want to look at them all.

MR. JUDISH: Well, I think the difference is that this is, you know, among other things, this is a database which Google has free access and free rein to, and so it's entirely appropriate in a context where Google operates freely within a database to -- for it to have Google go through and make a very -- to search through it and -- search through it not in the Fourth Amendment sense, in the computer science sense, to look through the database in order for that -- to find that narrowly targeted information.

A couple of points on this. You know, this is not an entirely new thing. I mentioned in our brief the *Ameritech v. McCann* case. I think a subpoena for the phone records of everyone in the

country would be a very troubling subpoena and overbroad under almost any circumstance you can imagine. However, for decades, you know, because phone companies store local calling information, index it only by the outgoing number and not the incoming number. When they receive a subpoena asking them who called -- you know, if they asked, like, "Who called Nathan Judish?" They have to look through their entire database and sort through that entire thing in order to get the limited information about who actually did that.

So searching through a giant database to find limited information is not a new thing. *Ameritech v. McCann* is not about a Fourth Amendment challenge. It's about who pays for that, whether the government's on the suit for the cost. No one has thought that there's a Fourth Amendment problem with looking through the huge database in order to get this very narrow targeted set of information.

Also, you know, another point that comes out of *Smith v. Maryland* is that Fourth Amendment protections really should not depend on a service provider's internal business practices which are not visible to the public.

THE COURT: Not -- I'm sorry?

MR. JUDISH: Which are not in any way visible to the public. And so in *Smith*, you know, the issue was whether it mattered that phone companies did not normally keep a record of the local phone calls that people dialed. And the Supreme Court says that doesn't matter. It has no constitutional significance. It would make a crazy quilt of the Fourth Amendment for that kind of thing to matter.

THE COURT: It would make it -- I'm sorry?

MR. JUDISH: A crazy quilt is the official term.

And so here, the fact that Google indexes its database like this is entirely invisible to the public. You know, as we've pointed out, Google could just as easily have stored this data in a different manner partitioned not by account but by location. The database would have the exact same information. It would search -- sorting through it would produce the exact same outcome from the government, and yet the Google's computers would not have to look at all the data at all. All they would have to look at is the data for whatever relevant partitions had the data for the geofence.

So the fact that this could be done without sorting through everyone's data strongly suggests that

there's no great Fourth Amendment significance to the fact that Google sorts through the data before turning over to the government only this tiny subset of the information. So, it doesn't make it a search.

I don't think I was searched by this geofence warrant. I don't think anyone whose information the government got back nothing from, I don't think the government learned anything about the rest of us. I just don't see how that's an invasion of a reasonable expectation of privacy when the government learns nothing about you. I don't think --

THE COURT: But that presumes that Google is not an agent of the government.

MR. JUDISH: I don't know if it presumes that or not. I mean, it's really -- it's -- I can't think of any case involving a search so insignificant that the Supreme Court would think of that as a search. What you learn is just so -- I don't even think you learn anything.

THE COURT: Well, they say what you learn is an anonymized number that's static that is a person or an account. And so you can readily with a subpoena find out who that is. So you're learning something, they're saying.

MR. JUDISH: We learn something about those

19 accounts. It is, to some extent, anonymized, but I'm talking about the supposed tens of millions of other searches. Those we learn nothing about. And so that's what I'm saying I just don't think that has any Fourth Amendment significance.

The defense now -- a lot of its argument is about all the people who have location history about whom the government learned nothing, not an anonymized account number, not whether they exist or not, nothing. We learned information about 19 accounts. I think it's fair to debate whether that's a search or not. But what did we learn about those supposed tens of millions? Where was the invasion of privacy when the government learned nothing? And Google learned nothing that they already didn't know. There's a giant database which they search through anyway. They didn't learn anything from it.

So, I want to go to the discretion issue associated with the warrant. The first thing I would say is this warrant just left no discretion whatsoever to Google. Google did exactly what it was directed to. The warrant directed Google to disclose location information within a particular -- of devices which were present in a specified circle of 150 meters during -- in a disclosed two hours of location

information for them during the time of the robbery.

And Google had no discretion about what database it looked through. Google should look through every database it has which contains information which is responsive to the warrant.

THE COURT: All right. So you know what? I want to be sure we're paying attention to time. When did we start? 11:40. All right. We can keep with this discretion issue, and then we'll probably take a break.

MR. JUDISH: So, Google did what they were directed to do. And everything they did is what the warrant directed. So, it isn't --

THE COURT: So, Mr. Judish, you have to address more specifically what they said. Right? So you can say Google did exactly what it was supposed to do. Right? So that's fine. But they don't say that. So you have to tell me why they're wrong.

What they say is that it just said search your databases, and somehow Google only searched Sensorvault. And there's nothing on the record that says why didn't they search Web & App Activity. Right? So they're saying somewhere there's discretion there or an agreement, but nobody knows where.

MR. JUDISH: Sorry, Your Honor. There is

stuff in the record. What's in the record is McGriff saying that the Sensorvault database is the only database which contains sufficiently granular information to be responsive to the warrant.

THE COURT: Sufficient what information?

MR. JUDISH: I don't know the exact words, but he says both in his -- that it's the only -- it's the only database with sufficiently granular information to be responsive to the warrant. So that's why they don't search the others.

As a recipient of compulsory process, they're supposed to, you know, know what they have that's responsive. As a -- someone who helps prosecute other cases, I was hoping we'd learn in this case that they had more information that they hadn't been disclosing to us that would be helpful in other investigations. Turns out, according to McGriff, they don't have that information. So what else -- if there's nothing else responsive, then they've done their job pursuant to the warrant and disclosed what they were directed to disclose.

THE COURT: So you're saying it's okay that Google knows that, but that the government doesn't know that they have only searched one?

MR. JUDISH: I'm saying that it was

appropriate for Google to do what the warrant said and give all the information they had about information which falls within the scope of the warrant. And Google -- the providers always know their databases best. And so the warrant is very specific about information it wants. And so Google, then, should look through all the information it has. And it's okay for Google to know that and not us. I mean, they don't always tell us everything --

THE COURT: So do you think that the phrase "sufficiently granular" is at all subjective?

MR. JUDISH: I mean, the -- that's McGriff's testimony. He says there aren't other databases which are responsive to the warrant.

THE COURT: Well, he says that aren't sufficiently granular. So how do we test that?

MR. JUDISH: Well, I mean, Google receives the warrant, and it complies. I mean, I think that he explained that it would be like databases which would tell you that someone is in Richmond. Obviously, a database that tells you some information that tells you someone is in Richmond isn't going to be responsive because it's not going to place someone in this circle.

And so the warrant itself is quite clear. We

want information about, you know, where you can -- about location within this circle. And so Google had, and apparently complied, with its obligation to go look at whatever data it had which could place someone within a circle like that. So --

THE COURT: And so neither the magistrate nor the agent needs to know that?

MR. JUDISH: No, I don't think so, Your Honor. We know that Google has location information. And so like Google's internal names for it and things like that, I don't think that's critical. Whatever information they had which can place someone in the geofence is going to be evidence of crime, and it's appropriate to ask them for that information.

So as far as the three-step process goes, do you want to take a break before we move on to the discretion associated with the three-step process or shall we continue?

THE COURT: You know what? I think we should take a break. So it's now twenty of one. We should take a 40-minute break so people can eat if they want to. So we'll go until 1:20. All right? We'll take a lunch recess.

(A luncheon recess is taken from 12:40 p.m. until 1:25 p.m.)

THE COURT: All right. Mr. Judish, I'm not sure if this gets to what you're going into, but I am going to just be sure that I've covered the questions that I think pertain to what you just argued.

So I spoke to you about sort of the frequency with which Google updates and stores the information, and I used two minutes. I think that's on the record, but I know that in our data return it was as quick as 30 seconds.

So in response to my question, you said, "I don't think it would matter to users if they knew it was every two minutes." So I'd like you to address the evidence that I saw and heard that Google was concerned about that. The emails that said, "Count me among the Googlers that had no idea we were doing this." And that Google actually changed its policies as far as notification because, in part, of that process, which all happened after Mr. Chatrie's case as far as I know.

MR. JUDISH: Your Honor, I think it's hard to attribute the specific changes in Google's terms and service and banners and all that to any specific thing. I mean, McGriff explained there was an ongoing process and a continued attempt to improve their process. So I just don't think you can draw any

particular inferences on any particular language from anything in the record.

I do think that it's just -- the thing to look at is -- you know, one way of looking at it is do what people do fall within the scope of the consent given by people who opted into it. You know, "saves where you go with your devices" really means saves where you go with your devices. And so whether it is, you know --

THE COURT: So it's not -- even though Google employees who work for the company that said "saves where you go with your devices" were surprised, that doesn't matter?

MR. JUDISH: I mean, there's a lot of employees who work for Google. There's a lot of people in the country, but I think the real question to look at, that we normally look at in Fourth Amendment consent situations, does this fall within the scope of the consent. And if you say "saves where you go with your devices," then you agree to that, then Google can save where you go with your devices. There is, you know, in the world of computers, lots of data gets generated in almost everything we do. To me, the unremarkable thing about this case is just how little data the government obtained.

THE COURT: You're going afar from what my question is. So you're saying that it's within the scope of the consent because this one sentence was enough, and it wouldn't have mattered if you said it is updated every two minutes because it's incorporated within that sentence, and it wouldn't have mattered as far as it being consent that it was updated every 30 seconds because it's incorporated because "Saves where you go with your devices" says "Saves where you go with your devices."

So what do I do, if anything, with the reality that no one reads that stuff? Nobody reads the privacy policy. What do I do with that?

MR. JUDISH: I mean, courts do pay attention to privacy policy (unintelligible) --

THE COURT: You definitely have to speak up. I don't know if the microphone is too far away from you or what.

MR. JUDISH: I'm sorry.

Courts certainly do pay attention to privacy policy in terms of service. The *Adkinson* case in the Seventh Circuit is an example of that. But this is more than just an obscure privacy policy thing.

The noteworthy thing about the opt-in process is how it is done through a relatively small amount of

text that Google has worked hard to get people to read. It's not long. "Saves where you go with your devices." This isn't a case where you're getting bogged down by, you know, those gigantic scroll-down-click-through things that we often have to look at.

So, I mean, I don't think it's fair to assume that people won't actually read that one little sentence before they agree to it. And, I mean, in any case, people are generally bound by their agreements, but Google really does a much better job than most other providers in getting people to agree to terms of service in trying to do this in a way that people will actually read and pay attention to.

That's one thing I took away from the McGriff testimony is they're trying hard, and they have done a pretty good job, I think. If I were to sit back and try to think what will people actually see? It's not the wall of text. It's something like what Google did here with the, like, "Saves where you go with your devices," and like one or two or three other lines for further explanation. And then if people want more, it's available. That's pretty good.

THE COURT: So tell me -- I mean, it doesn't matter whether you and I think it's good. The

question is whether or not it's constitutional and appropriately giving notice.

So where is an individual on notice about how precise the geolocation is? So one issue is if you're getting a phone number, right, you're getting a phone number. But we heard testimony that this location can be as specific as within 2 meters. So if you're getting updated every two minutes, if it's two minutes, I mean, our return had some that were 30 seconds, if you're getting updated every 30 seconds within 2 meters, are you saying that's not qualitatively different as far as a notice and an opt-in process? Where does it say we know exactly where you are?

MR. JUDISH: Well, there is mention in GPS data somewhere in all this. I'd have to look to see where it is. But people know that GPS is accurate to within a few meters. And there's mention of Wi-Fi. I don't know if it's as readily known, but people who know anything about this know that Wi-Fi is accurate, but not as accurate as GPS, but it's still reasonably accurate. And also it says because -- and this is, again, quite remarkable. Google says from the little opt-in screen "You can review your data" and it gives you a link. And you can go and you can actually see

the data. So that's distinguishes it from the information stored by phone companies. And even in the *Smith* days, you didn't know what data you had. Here you really can. Google will tell you every bit of data it stores about you. You can download it all in one piece if you want and take a look at it or you can look at it online. So Google's not hiding the ball.

THE COURT: So most of the GPS cases that I am aware of that say it's constitutional involve instances where folks are being followed on public roads. So I think what the defense is saying here is that one of the issues is that this GPS data, or whatever it is, within 2 meters can include constitutionally protected spaces like a church. So that's what I have in front of me.

They're not claiming that we found Mr. Chatrie in his house. But they're saying he was in a church. You can't do that.

MR. JUDISH: Again, Your Honor, I think I covered this point before, but *Knotts* and *Karo* are about surreptitious tracking. They're not about information disclosed to a third party.

In *Smith v. Maryland*, that involved a landline telephone. There were people sitting in

their house making phone calls. You can place a person, in those days, on a call on a landline phone also within a few meters, because how long were the phone cords? Not that long, typically. But in any case, they certainly placed people within a private space. And the Supreme Court said it didn't matter, that you could determine people were in their home within a private space because the person was disclosing the information to a third party.

And here people are choosing to disclose their information to Google in order for Google to provide them with location-based services. So it doesn't violate the Fourth Amendment when Google then shares that information with the government.

THE COURT: So if you're making a phone call out of your house, you're in a private space. So I guess if you make five phone calls in one day, the government is aware you're in your house five times in one day or at least a phone number is being dialed out in one day. But with respect to most of the tower dump cases, right, isn't it the case that it's not seeking a single data point, right? It's like watching a phone go down a street. Am I right about that? So you're going to different towers?

MR. JUDISH: Most of the published cases have

involved searching multiple towers. Certainly not all tower dump cases are like that. Sometimes we're just interested in dumps at a particular place and a particular time.

Mostly that's going to be useful if there's, you know, a place where there's not a lot of people. I remember one case that I consulted on, someone had dumped a body in an obscure location sometime between midnight and 6:00 a.m. In that case, a single place tower dump would be helpful.

THE COURT: Right. So when you get a tower dump, is it the case -- and I guess I want you to compare what's happening in this with us here.

So I think what you're saying is Google looks at not tens of millions, but lots of records that the government doesn't really see. Do they disclose the bigger amount?

MR. JUDISH: No, Your Honor, not at all.

THE COURT: Stage I is not disclosed at all?

MR. JUDISH: Stage 1, we get information about the 19 individuals who had data points present in the geofence during the hour of the bank robbery. That's it. They don't give us any information about tens of millions. We don't know how many people there are. We don't know how many people have location

history enabled or anything like that. All we get information on is 19 people. There's nothing beyond that.

THE COURT: So if you're getting a tower dump, when you're dumping the towers, are you getting just the 19 people three times or are you getting everything on the tower? Is the government doing the comparing?

MR. JUDISH: The government does the comparing on tower dumps. So typical tower dumps often involve hundreds of thousands of records. So that's why, as we explained in our briefs, this process -- the geofence warrants tend to be much more limited than a tower dump because in tower dumps, we actually learn information about a lot more people being in the vicinity for each tower dump we get.

THE COURT: But that discounts that Google is looking at that information, right?

MR. JUDISH: Yes.

THE COURT: They're saying Google is the agent. So the government is getting information. They're just only turning it over to another part of the government, the 19 names?

MR. JUDISH: I would not say the government is getting any information about those other people.

THE COURT: I know you wouldn't say that. That wasn't my question. My question was, they're saying that Google is the agent, and so when they're looking at those, that they are at least accessing information about numerous individuals.

MR. JUDISH: Yes, Your Honor. I would note that Google accesses that information anyway. That's how their system works. So Google isn't learning anything it wouldn't use or didn't already know.

It's in their Sensorvault database, which they access frequently for whatever purposes they have. They're looking to try to do what they call semantic information, being able to analyze someone's location history to determine things which would be useful for Google for advertising purposes and stuff like that. So Google looks through the location history. So it's --

THE COURT: So are you saying that Google does that through separate searches, that it's not an algorithm that just works that out? This is different, isn't it? I mean, Google doesn't go in and say, or do they, who is near the federal courthouse so that I can advertise, as a lawyer, on average in a particular period of time?

MR. JUDISH: I think that's exactly what you

can do if you want. That's what Google calls radius targeting. You can say I want --

THE COURT: You can't say "you." You have to say who can say, who's controlling it.

MR. JUDISH: Sorry. An advertiser can say to Google, "I want to target people within a kilometer of the federal courthouse." And then Google will target ads to those people. Google describes this process on its website.

And then afterwards, if you have your law office at some particular place, Google will then do a geofence of people who visit your law office to see those people who it targeted advertisements to, which of them subsequently visit your law office. And then it will tell you how many there are in that. So that really requires Google to do a geofence of people visiting your law office. You know, it's checking to see of these people who they targeted the advertisements to, do they later visit this very specifically defined location. So it's really very closely related to what is done here with a geofence warrant and --

THE COURT: You keep referring to the *Smith* case, and I may not be remembering it well, but didn't the *Smith* case involve use of an operator?

MR. JUDISH: No. No, Your Honor. I mean, it would have been an electronic pen register device in *Smith*.

THE COURT: Okay. All right.

So I'm just going to ask you to address as you go forward, *Carpenter* is focusing on what reveals the privacies of life, right? So I want you to use that lens as you describe to me how you're going through the stages.

MR. JUDISH: All right. So I just want to put on the record one citation before I move on to the three-step process. We talked about where Mr. McGriff explained that location history was the only information sufficiently granular to respond to a geofence warrant. You can find that in his first affidavit, which is Government's Exhibit 3 at paragraph 20.

So the three stages, the three-step process, the first thing I'd say is that I actually, you know, as the Magistrate Judge Harjani in Illinois explained in his opinion, the multi-step process really does lack constitutional significance.

I mean, the key thing here is that we establish probable cause and specify with particularity for all of the information that we

potentially could have obtained. Google very much likes the three-step process. And I think it's an affirmatively good thing that has some additional ability to provide sort of practical privacy protections while still enabling our investigations to proceed. But that doesn't mean that it's constitutionally significant. That's exactly what Magistrate Judge Harjani said. You know, it could have practical benefits, not constitutionally significant. But the key issue before this court is whether the issuing magistrate had a substantial basis for his determination that the evidence the government could potentially obtain was, in fact, evidence of crime and for that reason it established probable cause for it.

But anyway, the way it works is that the first step of the three-step process, all that we got pursuant to that is the latitude and longitude coordinates, which were in the specified geofence, the circle with the radius of 150 meters.

THE COURT: You just, you know, you have to be slower. You just do. Because I don't know what those numbers were. I read them, but our court reporter has to get them as you say them.

MR. JUDISH: All right.

All we get from the first step of the geofence is the latitude and longitude coordinates, which actually fall within the geofence during the hour of the robbery.

So if people, to the extent people came and went from outside during the Step 1 information, we don't get that. It's just if the latitude and longitude points in the Sensorvault database fall within the circle during that hour, then we get those along with an anonymized reference number from which we cannot, without more from Google, determine any identity information.

So that, you know, as far as privacy of life goes, I just don't think that's all that private. Certainly going to a bank is not a particularly private activity.

I do feel obliged to note that I don't think that -- to say *Carpenter* is about protecting the privacies of life, it can't go that far. You'd have to overrule *Smith* and *Miller*. Who you dial on a telephone, that's private. Your financial transactions, those are private things. I think we really do have to take *Carpenter's* word that it's about long-term location information.

But anyway, addressing the Court's question

as to how private the information is, your presence in that 150-meter radius, I think, is not all that private. Obviously, there is a church there. It is hard for me to believe that one can protect oneself from a bank robbery by choosing to rob a bank next to a church and using the church parking lot. And there, I guess, I would point to the Fourth Amendment principle that you can't rely -- it has to be about violation of your Fourth Amendment rights. You don't have standing to challenge Fourth Amendment violations of others.

And whatever the defendant was doing the day of the bank robbery, I don't think he's claimed that he was going to church. So he -- so I don't think that has any impact --

THE COURT: Does he have to claim that? What's his obligation?

MR. JUDISH: I mean, if the issue is to try and assert that his privacy interests were invaded, he needs to explain how his privacy interests were invaded. And so that's the issue which I think he fails on because the defense keeps talking about the potential privacy invasion of people being found inside their home. They don't claim that he was found inside his home. They talk about privacy issues

associated with church. They don't say he was associated with church. He's got to claim his privacy invasion, that his privacy interests were invaded.

So one case I can cite on that is the Seventh Circuit case *Patrick*, which involved use of a cell-site simulator to locate the subject of an arrest warrant. And *Patrick* tried to claim that use of the cell-site simulator violated the privacy interests of others nearby because the cell-site simulator, which is a device which has essentially a direction antenna, which locates where nearby cell phones are, violates the privacy of others nearby.

The Seventh Circuit says no, under *Rakas*, you don't have standing to assert any privacy violations of others.

THE COURT: So are you saying that factually Mr. Chatrie was not in the church?

MR. JUDISH: I don't -- to my knowledge he parked near the church. I have no knowledge that he was in the church. I don't know of anything in the record on that. I mean --

THE COURT: Was he within 2 meters of the church?

MR. JUDISH: He may have been, Your Honor. I don't think -- I think there may be stuff in the

record. I think his coordinates are plotted. And so that would be the place to look for that. I can't state with certainty. So that's the first step.

The second step of the warrant, you know, that enabled the government to get all of the location history over a two-hour interval of the individuals whose information was disclosed in the first step. And so that does, you know, potentially implicate greater privacy interests because you can't have people going to and from the area. But, again, I don't think Mr. Chatrie has pointed out any particularly heightened privacy interests of his which were infringed.

And in any event, I think the real issue is, was there a substantial basis for the magistrate's determination that this would be evidence of crime? And, you know, the additional contextual information is extremely helpful in showing what people's roles in the criminal activity was. And so it was evidence of crime, and therefore appropriately fell within the scope of the warrant.

THE COURT: And so I may be getting ahead of where you are about to argue, but explain to me -- my understanding is that with this degree of certainty of the radius, there is a 150-meter radius, but then a

broader radius that may actually be implicated. Am I right?

MR. JUDISH: Google has, you know, there's chance for errors in the data. There's no question about that. The warrant directed Google to disclose the points where the points calculated by Google fell within the radius, but there was certainly some chance of false positives in that. And, again, I just think that that would go to the weight given the evidence as opposed to whether or not it is actually evidence of crime.

THE COURT: Well, what they're saying is one of the issues is that if you're signing a warrant -- I mean, I think they say it's almost twice as much, like 378 meters, 387 meters, that a magistrate is not on notice that it could be actually twice as large, the area that you're searching, given the rate of potential certainty.

MR. JUDISH: First, I just want to go into the facts. I think they significantly exaggerate the actual inaccuracy. There are a few individual points which have large errors associated with them, but if you look at the actual data, which is in the record, every single one of those will have another point for the same device with the same center and a much

smaller radius.

And as Agent D'Errico testified, what that actually means in practice is that the phone started at the smaller place and then went somewhere, and Google isn't sure where. So it's not that these are devices which may have been the whole time super far away. It's that the way that Google -- you know, they have indication that a device is on the move, but they don't know where. So they, you know, they keep estimating the same center point. But their uncertainty grows.

But the more general point, as far as the magistrate and what was in the affidavit, I think people understand that cell phone measurements are inaccurate, and, thus, I think a commonsense magistrate would know not every location information point is going to be perfect. So I don't think -- and I understand the defense has dropped its argument that it was a, you know, somehow a violation that we didn't include this information in the affidavit. I think that showed up in some of their briefs, but not their final one.

One other point I'd like to make about the three-step process is that it's clear from the Playpen cases that doesn't violate the Fourth Amendment if the

government chooses to obtain less than the maximum amount of information it's authorized to under a warrant.

In the Playpen cases, we were going after a child pornography website on the Dark Web, and we obtained a warrant authorizing us to use code to identify people who logged on to the site. We made explicit in our affidavit that we were authorized to use this code to identify anyone who accessed the site.

We, in fact, were likely to target our code more narrowly than that, and that's ultimately what we did. And this was challenged just as a vast number of cases -- I think there's over 100 Federal District Court cases and there are 11 Federal Court of Appeals cases dealing with challenges to this warrant. I don't think any court has found that that language was problematic.

THE COURT: Well, what is different, though, is that every person who logged on to that account violated the law 100 percent. So not 100 percent of people who were near the bank violated the law, like way, way less than 100 percent.

MR. JUDISH: Yes, that's absolutely right. But the key, what they have in common, is that there

was a substantial basis for the magistrate judge's determination that all of the evidence you're entitled to, all of the information we were entitled to, was evidence of a crime. And that's what counts. And so, again --

THE COURT: It counts because it was an illegal website. How is that not a completely different situation?

MR. JUDISH: Well, the warrants are used to seize evidence of crime, and that can be direct evidence that someone is guilty, but it can also be other information as well. And so the issue is whether a magistrate has a substantial basis to think it was okay or proper that all of the user location information we were authorized to seize would in fact be evidence of crime. It doesn't have to all -- all the people don't have to be guilty. The question is, is what we're authorized to get evidence? And here it was.

It's like I said. It gives us an ability to reconstruct the scene of this crime. It helps us identify accomplices. It helps us find witnesses. It's all appropriate evidence of crime, which can appropriately be seized pursuant to a warrant.

And, yes, there's not all criminals in this

case, but it is all evidence, and as long as we establish probable cause and identify with particularity evidence, I think it's entirely okay for us to then be selective within what the subset of what would establish probable cause and identify with particularity what we ultimately take away.

I think that happens, you know, all the time in search warrants is, you know, we have a warrant. You don't have to, you know, raze a house to find every bit of evidence in a house that you're searching even though, you know, you can keep looking harder and harder and find more of the key thing that you establish probable cause and identify with particularity the things that you are authorized to seize.

In any event, if the Court does have a problem with Step 2 of the warrant, I think the appropriate thing is severance. This is a warrant which is usually conducive to sever. The process was done. The language of the warrant is separate. The process is done in separate steps. This is a warrant which is just enormously easy for the Court to -- would be enormously easy for the standard severance doctrine to apply. From the Step 1 information in this case, it was sufficient to identify which account

likely belongs to the robber, and so the fruit of the poisonous tree would not extend to our subsequent investigation and all of the subsequent evidence we obtained in this case after we first obtained the geofence warrant information.

THE COURT: So you're saying because you had 19 names, you have had enough to identify Mr. Chatrie?

MR. JUDISH: Because we had 19 sets of location information in that 150-meter radius, and we could -- and from the other information obtained at the scene of the robbery, including surveillance videos and eyewitnesses, we knew where Chatrie had come from and, you know, parked, gone into the bank and returned. And the location information of Mr. Chatrie from the geofence warrant was sufficiently consistent with that testimony that we could still tell that he was the one, the robber.

THE COURT: So why did you ask for further information on all 19?

MR. JUDISH: I mean, there's other possibilities which need to be explored, ruled out, like having co-conspirators. And so I think that a lot of that is -- that is helpful to, you know -- investigators tend to be thorough. And they wanted to, you know, be able to get that information because,

you know, some of that information was not entirely inconsistent or, you know, some of that information, you know, suggested that it had some aspect that one might be a co-conspirator like, you know, data suddenly halting suggesting someone turned off their phone.

THE COURT: So, wait. I'm sorry.

MR. JUDISH: I think because there was a possibility of co-conspirators is one possibility to search or to obtain additional information.

THE COURT: So, I guess, then, I'm going to ask you, clearly the terms of the warrant said narrow it down, and your task force officer didn't. And then Google said you have to narrow it down. And explain to me what happened there.

MR. JUDISH: I mean, the warrant says attempt to narrow it down. And, you know, and we ultimately did narrow it down. And so I don't quite -- so, if you look at the actual execution, we did narrow it down. So I don't see any, as an initial matter, I don't see any significance with the, you know, with the fact that it was contemplated to obtain more than we actually did. I don't recall what was in the record regarding why we initially asked for all 19.

THE COURT: Well, I mean, there were other

things in the record like Google saying they didn't think the agent knew what he was doing. That's the only explanation we have it may be wrong, but that is in the record. So --

MR. JUDISH: I don't recall. I mean, I think it's really -- I'm not aware of the Fourth Amendment violation from contemplating but not executing a warrant in an improper way even if it would be improper.

THE COURT: I'm just trying to get the record straight.

MR. JUDISH: I'm sorry. I don't recall.

THE COURT: So how did we get to nine?

MR. JUDISH: Those were the ones which the agent thought were most -- the greatest continued relevance to the case.

THE COURT: And do we know why? Are there parameters that direct to the agent about why?

MR. JUDISH: The warrant very much leaves this to the government's discretion. And I say, again, I think these are of no constitutional significance. You know, part of the reason why is definitely the question of whether these people could actually be additional co-conspirators. And I think that's a primary reason for a continued look at other

suspects.

THE COURT: Okay.

MR. JUDISH: I'll turn now to good faith if you don't have further questions on the warrant itself.

THE COURT: If I do, I'll come back to them.

MR. JUDISH: All right. So, suppression, the Supreme Court has said, is a remedy of last resort and used only where its benefits outweigh its heavy cost. And what you have here really is a new investigative technique.

So when a new investigative technique comes along, there's not a lot of case law to look at because -- well, there's no case law to look at. And so what is an agent supposed to do?

And so the Fourth Circuit looked at this in *McLamb* in the context of the Playpen cases, and what the Fourth Circuit said is that in these, you know, the agent should consult with the expert prosecutors, and if they do that, then it's appropriate to apply in good faith.

Well, it's not because it's not -- they consulted with the prosecutors, and the prosecutors think it's okay. And then they also take it to a judge, and the judge thinks it's okay. And that's

exactly what Agent Hylton did in this case.

And I think it's worth noting, particularly in the context of you going to the state magistrate, that this was not the first time that Hylton had obtained one of these warrants. He had actually gone -- this was his fourth. It actually is in the record, and we've disclosed two of those warrants to the defense. The third remains under seal. That one hasn't been disclosed. But he had previously gone to both a United States magistrate judge and to two Virginia state judges, and they hadn't raised any problems with it. They had signed off on it.

So, what more can an agent do? The prosecutors have no objection to it, a federal judge has no objection to it, two state judges have no objection to it. At this point it's hard to understand why it would be objectively unreasonable for the agent to believe that it's appropriate to seek a geofence warrant.

That is exactly what the Fourth Circuit has suggested that he do. And in *McLamb*, and under those circumstances, suppression, the cost -- the harms of suppression will very much outweigh the benefits. If ultimately the courts -- other courts who look at this decide that it shouldn't be done that way, then,

obviously, it's going to stop.

That's what -- in the *Carpenter* case, that stopped the practice of using historical cell-site location information. But *Carpenter* himself, the Court did not ultimately suppress the cell phone location information obtained and used against *Carpenter* because of the good faith exception.

The benefits don't have to outweigh the harms when you're talking about -- in the context of new investigative techniques. It's also worth noting and closely related to this is we heard from Google more than 8,000 of these over the course of, I believe, a year. So it's clear from that the decisions made by the judges that Hylton has consulted with are not significantly different than the decisions being made by a whole host of other judges around the country, state and federal.

Or, alternatively, we can apply the traditional *Leon* good faith analysis to this. Under the *Leon* good faith analysis, there's no suppression if we rely on good faith on a warrant. And there's a few exceptions to that, but none of those exceptions really apply here.

And one is that the affidavit is so lacking in indicia of probable cause that reliance on the

warrant is unreasonable.

But there is probable cause here. We had a robbery. We had a guy with a cell phone. And the affidavit linked that directly to Google having evidence of the cell phone's location. And that establishes a fair probability that Google had evidence of crime, but it's certainly not wholly lacking in indicia of probable cause. So under the *Leon* good faith, the evidence should not be suppressed.

Similarly, in terms of particularity, the warrant is not so lacking in particularity that reliance is unreasonable. It specifies exactly the information that the warrant is seeking. The two hours of location information or devices which fall within this 150-meter circle during the hour of the robbery. And that's really quite particular. That's stuff that Google's algorithm can go through and separate. It's just -- it's not wholly unreasonable to think that as to a particular warrant, I mean, clearly, some variation of that sort of thing thousands of judges around the country are agreeing that it's appropriate. And at the time there was no contrary decision. And now we have just like a handful of those, like there's three or four

magistrates who have written on this, one of whom thinks it's wholly unreasonable, and others who sort of based on the facts of the case think the government should do a slightly better job. It doesn't suggest that there's anything wholly unreasonable about the government's reliance on the warrant in this case.

So, those cases, you know, generally suggest that, certainly the Weisman decision and the Kansas decision the defense just circulated, suggest that there's nothing fundamentally wrong with geofence warrants. The government just needs to be very careful about establishing probable cause in particularity.

By that standard, the warrant in this case clearly passes the good faith. I mean, the probable cause here is unusually strong because, you know, the robber was seen actually carrying and using a cell phone. That actually hasn't been the cases, in those other cases. They've just tended to make that assumption. But here we've actually got that. So it's just not wholly lacking in probable cause, not wholly lacking in particularity.

And similarly, there's no evidence here that the judge abandoned his judicial role. The judge did what judges are supposed to do. He reviewed the

affidavit and then he signed the warrant. I mean, the kind of case that the Supreme Court talks about for someone abandoning their judicial role is the case -- the example they give is *Leon*. And what that actually involves is a judge who decided to help with the execution of the warrant, that he actually went to the scene to be searched and decided what could and couldn't be seized.

Well, that's what the Supreme Court means when it says a judge who abandons his judicial role, you know, that you don't apply the *Leon* good faith. And there's nothing like that here. This magistrate reviewed the warrant affidavit and signed the warrant, and that's entirely appropriate, and so *Leon* good faith applies in this case.

And if you don't have any further questions, we'd ask the Court to deny the suppression motion.

THE COURT: I do have a question. I think I can discern from what you're arguing what case you think I should rely on for purposes of my evaluation of this case, but why don't you just tell me on the record.

MR. JUDISH: The Harjani opinion is one geofence case issued by a magistrate judge who bothered to write up his opinion, and I think that

there's a lot to commend that. And there's also the cell-tower dump. *James* is reasonable similar as a case, you know, at least involving evaluation of probable cause and particularity.

The District Court opinion in that case finds that cell-tower dump warrants are appropriate.

THE COURT: All right. So I think I've heard maybe both sides a little bit talk around or near or maybe directly suggest two things. One is that this warrant might be stronger if Google stored its information in a different way, if it was stored by location. So the question is, what's the upshot of that? Does any court have the power to say that? Would there have to be a congressional determination to make that happen? And I think I want to ask generally, I see that the government is steering away from the Stored Communications Act, and I want to confirm that you are resting this entirely on a constitutional analysis.

I mean, one of the issues is, of course, right, there is no statute that addresses geofencing. Right? And, in fact, there's been no statute addressing almost any more recent electronic surveillance process because it develops so quickly that almost as soon as something gets passed, say, in

two and a half years, it's obsolete.

So I want to hear what you have to say about what I have the power to do or the appropriate action I should be taking, and if there's any statutory obligation with respect to what's going on.

MR. JUDISH: I do think they'll start with the Stored Communications Act part. I do think this compelled disclosure of the information is governed by the Stored Communications Act. I just don't think it matters for purposes of a motion to suppress because the act itself has no statutory suppression remedy. And so it just doesn't matter.

Whenever you get into a Fourth Amendment -- the Stored Communications Act matters enormously --

THE COURT: Wait. You have to slow down.

MR. JUDISH: Sorry.

THE COURT: Okay. Just start right over and act like I don't know what you're about to say.

MR. JUDISH: All right.

The Stored Communications Act contains no suppression remedy. It contains a section 18 U.S.C. Section 2707, which specifies that the remedies in the statute are the only available remedies for the violation of the statute. And 2707 includes various damages provisions, but not a suppression remedy. And

there are various cases confirming, in fact, there is no suppression for a statutory violation.

And, you know, I think the *Smith* case in the Ninth Circuit, I think. Anyway, but here because the only issue for this court is whether the evidence should be suppressed, the Court just doesn't need to focus deeply on the questions of how this information falls within the --

THE COURT: Does it need to or can't?

MR. JUDISH: I'm not sure why it would be relevant. I mean, you certainly -- I'm never going to tell a judge what it can or can't do. But I just don't see the relevance to this case. I mean, sometimes we can argue that that's an additional reason against suppression. But, you know, like a good faith reliance on a statute. But here the government has not advanced that position. We have argued good faith based on *Leon*.

So -- and as far as the structure of Google's database, I don't think, you know, I never want to willingly waive the government's authorities or powers, but I'm certainly not in a position of making any claim that a court has authority to tell them how to structure their database.

I think the main argument that we make based

on the structure of their database is the argument that Fourth Amendment rights should not turn on internal prior practices which are not visible to the public, and the structure of their database is one of those things. And, thus, the fact that this could be done in a way which would allow Google to -- Google's machines to filter very narrowly, strongly suggests that there is no search of millions of people when its database requires a broader filter.

THE COURT: And with respect to -- does the government have any position about whether or not a review at each step by a neutral magistrate would be necessary or beneficial or better?

MR. JUDISH: I mean, I think if we can, as I believe we did here, establish probable cause for all of the evidence from the start, it's fine to do so. I don't think it does any harm to have additional steps. It could be structured to require to have a magistrate make an additional finding along the way, and there would be no problem with that.

So I think it's not necessary, but not in any way problematic to involve a magistrate in multiple decisions.

THE COURT: Right. And so if -- I guess I want you to unpack exactly why the ability to delete

the information, if Mr. Chatrie could figure that out, how it affects my analysis.

MR. JUDISH: I think one way it affects your analysis is it distinguishes this from *Carpenter* and why *Carpenter* said the third-party doctrine didn't apply. *Carpenter* had three reasons for why third party didn't apply to cell-site information. One of them was that it could be deleted.

THE COURT: All right. And so I'm not quite sure how to phrase this, but -- so if there's probable cause here, obviously, there's video surveillance that a robbery occurred. Is the government's position that there would still be probable cause to do this geofence if there were no video or any indication that Mr. Chatrie had a phone?

MR. JUDISH: It can be. I mean, cell-tower dumps in the *James* case, for example, there was no evidence that the defendant had a phone, and the Court still found that probable cause was established. I mean, probable cause is a common sense determination by the magistrate whether there's a fair probability that the target had prior evidence of crime. And so you certainly can have that.

In another of the cases, I think the Harjani opinion, that involves criminal activity of the sort

that it looks like it was probably more than one person involved, and so that gives rise to an inference of a likely cooperation among people, and people use cell phones to communicate and cooperate. So you have to look at the facts of any particular case and make a determination of whether they establish a fair probability.

So sometimes I think you can establish probable cause regardless of whether a person has a phone. It's really --

THE COURT: So I guess I'm trying to find out where it stops. Like when don't you have probable cause if you don't have evidence of using a phone, probable cause for a geofence?

MR. JUDISH: I think it's really -- it's -- I think it just depends on the facts of the case and whether you think there will be evidence of crime. And this is a determination made by magistrate judges. This court obviously doesn't need to confront that in this case because this is a case with a cell phone. But I do think that, you know, the fact that if there really is, you know, a fair probability that Google will have location information of someone who committed a crime, a warrant should issue, and it shouldn't be an argument that, well, that happens a

lot. It is true that we're able to solve lots of crimes because we establish probable cause in lots of circumstances. That is an affirmatively good thing.

So I don't think that an argument I've seen from at least one magistrate judge in the recent Kansas opinion that we can't have too many of these geofence warrants is correct. I think the issue is, can we establish probable cause? And you can't say this isn't probable cause because you're going to solve too many crimes that way.

THE COURT: I think that's a little different from saying when isn't there probable cause, right? I mean, no one is going to say let's not solve crimes. Right?

MR. JUDISH: Right.

THE COURT: Defense counsel is not going to say that. That's not what they're arguing.

MR. JUDISH: I apologize, Your Honor. I guess the way I should say it, the Court seems to think that warrants shouldn't issue because they would issue in too many cases, and -- but that's not --

THE COURT: I'm not asking that question. I'm asking when doesn't it issue? I'm saying, give me an example.

MR. JUDISH: I mean, there's -- I mean, I

guess you could have an example where it's clear that a guy wasn't carrying a cell phone. You know, if someone walks in with, you know, pocketless gym shorts and a T-shirt and commits a crime, you can probably tell by looking at him or from video surveillance footage that there is no phone on this guy. And in that case, I think there wouldn't be probable cause.

THE COURT: All right. Okay. I think that's it.

MR. JUDISH: All right. Thank you, Your Honor.

THE COURT: Can I ask you how long you think your response is going to be?

MR. PRICE: I will try and keep it very brief, Your Honor.

THE COURT: Well, that is about as particular as whether it's granular.

MR. PRICE: Sorry about that. I have three points. I think less than 10 minutes.

THE COURT: Okay.

MR. PRICE: Counsel tells me maybe 15.

THE COURT: Maybe 15. All right. I'm going to give Ms. Daffron a little bit of a break. I just think that, you know, maybe she'll buy me a cupcake after.

All right. We'll take a 15-minute recess.

(Recess taken from 2:22 p.m. until **2:40 p.m.**)

MR. JUDISH: Your Honor, I just want to make -- correct the transcript in one place. I did not do a great job explaining this.

THE COURT: That's fine. Please approach the podium to do that.

MR. JUDISH: Thank you, Your Honor.

Regarding the reasons behind the second stage of the search, they are explained by Agent D'Errico at page 546 of the transcript. So I'll stop there.

THE COURT: Wait. I'm sorry.

MR. JUDISH: Okay. So -- all right. I won't stop there.

THE COURT: Yes.

MR. JUDISH: So, Agent D'Errico was asked why go back at the second stage. And at 546, he says there are several reasons. I know I need to talk more slowly. I'm sorry.

So the first reason is, this is a device that was present in the area of the bank prior to the bank robbery. And we know that sometimes when people want to hide their location, they will turn their phones off. And if their phone is turned off, no additional location history would be reported for that device.

So it's significant to us that there is a point inside the geofence that occurred prior to the bank robbery with no points after the bank robbery because we also believe that after a subject has robbed a bank, that they are going to flee the area and not have any additional location history records within the geofence several minutes after the bank robbery.

THE COURT: All right.

MR. JUDISH: That's all, Your Honor.

THE COURT: All right. Thank you, sir.

MR. PRICE: Good afternoon, Your Honor. Can you hear me okay?

THE COURT: I can.

MR. PRICE: All right. I'd like to begin by correcting a few points for the record.

The first is that radius targeting, which is that form of advertising the government was talking about, does not use location history according to Google.

THE COURT: Wait. Say that again. Radius --

MR. PRICE: Radius targeting, this idea that you can advertise to everybody around the courthouse if you're a lawyer. While that may be possible, Google has stated -- it's at page 197 to 98 of the transcript -- that location history is not used for

that purpose.

Second, with respect to traffic predictions, once again, pages 407 to 408 of the transcript explains how Google does not use location history but uses aggregated data and percentages with added, quote, noise to prevent any possibility of ID'ing individual devices.

And then, finally, with respect to the questions about how the government narrowed things down in Step 2 and then Step 3, we should note that one of the three finalists, so to speak, was, in fact, one of the false positives. So somebody who was just driving by, likely never within that geofence at all, and was reported as being inside of it, therefore it had Stage 2 data under the government's reveal, and then Stage 3 data as well. That was one of the false positives.

THE COURT: Okay.

MR. PRICE: So I want to touch briefly on a few points.

First, this idea that location history is voluntary because of the process involved, and the mere fact that it is stored with Google, a third party.

Almost everything the government said about

the voluntariness of enabling location history can be said of Gmail, of Google email. It is stored by Google. It is transmitted by Google. Google advertises off of emails. And yet even the government agrees that email deserves Fourth Amendment protection. I suppose they have to after the Six Circuit's decision in *Warshak* and their representation to the Supreme Court in *Carpenter* that email requires a warrant to get.

That is not something that the Supreme Court has weighed in on. And under a strict reading of the Stored Communications Act, as it still exists, the government did, in fact, argue they did not need a warrant to obtain email that was older than 180 days.

The Sixth Circuit in *United States v. Warshak* found that email, despite being housed on Google's servers or on other servers, deserved the same kind of privacy as one's papers and effects. That is the modern day scion of one's private papers and effects.

All of those points we can attribute, as well, to location history. The Stored Communications Act, while not determinative, is certainly relevant to the reasonable expectation of privacy analysis.

Google considers location history to be content and users understand that content is their

data and it is protected from unauthorized disclosure.

Likewise, this is different from a subpoena, fundamentally different from a subpoena, because Google is not searching its own business records. The government is not asking to search preexisting records that Google already has in the same way that a cell company might have data about how many people use a tower in order to figure out whether to add another tower or why calls might be getting dropped.

Google never runs a search to figure out who was around the bank or who was around. They don't have towers. They have no need for this, to have location data sorted by location. It is considered, once again, user content, and that is why the database -- the Sensorvault is structured in that way. It is a reflection of this idea that location history is content. It belongs to users. It is their data. They can manipulate it. They can delete it. It is not Google's data.

I want to touch briefly on the idea that *Carpenter* hasn't been applied or expanded since *Carpenter* was decided. The government cites *Hammond*, which is a case about realtime cell-site information, as well as historical cell-site information; 127 days of it actually. And there the Court found that a

search of the 127 days of historical cell-site information was a search, but that the good faith doctrine applied. Why? Because the 2703(d) order was issued prior to *Carpenter* being decided.

So, in fact, the vast majority of cases that have been decided since *Carpenter* follow a similar pattern recognizing that these cases take some time to percolate up. And some of the searches that we're still seeing right now were executed prior to June of 2018.

So those cases are just coming up now, and the vast majority of them holding that *Carpenter* doesn't apply do so on good faith grounds.

The other case that the government cites, also a Seventh Circuit case, *Adkinson*, did involve a tower dump, but the government didn't conduct it. The suspect in that case, the defendant in that case, was accused of robbing multiple T-Mobile stores. So T-Mobile, on its own, looked at its own cell-site records to try and figure out which T-Mobile customers had used their towers near those stores. So it wasn't government action in the same way that we have here.

And I think that leads in nicely to this larger point that Google was acting as a government agent. There would be no Step 1 data without Google's

participation. And Google would not have done any of this had it not received compulsory legal process. Google, in this sense, can't be anything but a government agent at Step 1. The government is outsourcing the search function to Google. It's that simple.

Finally, I want to touch on the *McLamb* Playpen good faith argument. As Your Honor correctly pointed out, that case turned -- was based on the fact that there was probable cause for every computer that was searched. So the issue there was not probable cause. The issue in *McLamb* was a very complicated jurisdictional question about the reach of Rule 41 and whether judges in one district could issue warrants that applied extraterritorially to other jurisdictions.

At the time there were multiple conflicting court decisions in the country about this. And it was, admittedly, something of a close call. So in that case, consulting with attorneys and prosecutors would make a lot of sense. But there was no question about whether probable cause was necessary. That is a fundamental question, a fundamental Fourth Amendment question that has to be answered in every single case. And it is antithetical, I think, to the Fourth

Amendment to say that the government can get away with a warrant that doesn't have probable cause or lacks particularity simply because they checked with the prosecutor.

That rule, if read that broadly, would eviscerate the Fourth Amendment. Anything that a government agent wanted to do, they could just clear with the prosecutor, and so it would be good faith at the end of the day. I don't think that's the rule in *McLamb*.

Once again, the Court was not looking at a basic question like were these warrants supported by probable cause. It was a very technical, legal question about the reach of Rule 41.

THE COURT: Well, to be clear, they're saying that, regardless of anything in *McLamb*, they had probable cause here because they had a video of somebody robbing a bank using a phone.

MR. PRICE: I don't think that having a phone in and of itself is enough to establish probable cause. If only a third of Google users have location history enabled, and not all people who have cell phones have Google phones, and some of the people who, because of the way that the 68, 32 percent error rate works, at least some of those people who might have

been there will not show up there within the geofence because of this idea of false positives and false negatives. So I think there's actually a few more steps to do to go from having a phone to probable cause.

And as we know from *Riley*, and the government's own statistics, having a cell phone is a fairly common thing. And I have no doubt that in a case where the suspect was not seen with a cell phone, perhaps wearing gym shorts and a T-shirt, that the government would say he left the phone in his car or that they might need to get a warrant or look for witnesses or co-conspirators anyways.

I think there is a lot of work to be done on the probable cause front to go from a cell phone was seen to there's probable cause for searching location history.

THE COURT: Okay.

MR. PRICE: That's all. Thank you very much, Your Honor.

THE COURT: I'm going to ask you one question based on their argument. It seems that part of what they're saying is that the probable cause was based on the fact that there was a crime and that getting the results of the geofence would help reconstruct the

crime. That it's just an investigative tool. And so there's probable cause to know that the way that folks were operating around, it's just a different type of surveillance, and that it would, at least probably, show evidence that a crime had been committed.

MR. PRICE: I think there's a lot of information that might be helpful in the abstract. And nobody is preventing the government from obtaining this information. The idea is simply that they must have probable cause to do it.

So it may be useful to get the location history data of people inside the bank, but then identify those people inside the bank and seek a warrant for their location history information if all you're trying to do is just get a better sense of the scene. In the same way that you would go and identify the surveillance cameras in the area and get the video from there, you wouldn't start with every surveillance video camera in the country, and then narrow it down to the ones around the bank.

So I think while there may be lots of information that's useful in terms of solving crimes, the Fourth Amendment limits what the government can get based on probable cause and particularity. Thank you.

THE COURT: Thank you.

All right. Well, I want to thank you all for your efforts and for your argument.

I am, not surprisingly, going to issue a written opinion. You all have submitted lots of documents, and I've heard testimony, and I want to be sure you have a decision that you can read and either agree with or disagree with, and then move on from there.

I certainly will do so as swiftly as I can. And, certainly, we've been working on it, and we will continue working on it. So we're not behind the ball, but we're not where you guys are. We haven't finishing our briefing.

So how is it, with that understood, how is it that you want to proceed?

MS. KOENIG: Good afternoon, Your Honor.

THE COURT: Good afternoon.

MS. KOENIG: I think Ms. Daffron is probably grateful that I wasn't talking very much today.

But I think in terms of the defense perspective, obviously there are other motions that are pending. I will say that the Court's determination of this motion, I think, will make dispositive some other issues in the case regardless

of how the Court rules.

So from the defense perspective, I would ask that the Court continue to hold the other motions in abeyance until after the decision on this motion. I don't believe at this point we need to reset a trial, but if that becomes necessary, obviously we can do that once the Court makes a decision.

THE COURT: Right. Does the government have a perspective?

MR. SIMON: Judge, we don't mind the Court holding those motions in abeyance. To the extent the Court wanted to rule from the four corners of the search warrant, I don't believe we intend to elicit additional evidence on those motions. So we'll just defer to the Court on whether it holds it in abeyance or not.

THE COURT: All right.

Well, what I will certainly do is not rule on those issues without notice. I think that's fair. And so I will decide this particular motion, which is clearly the heart of what we're discussing, and then we will handle the other motions accordingly, but not by surprise. So you can presume that I would handle it that way.

I'm not going to schedule a trial date. So

this means that this motion is under advisement, including all the findings that I've made with respect to the complexity of the case, the fact that we've had testimony from across the country, unusual sets of affidavits.

It is the fact that the speedy trial continues to be held in abeyance for a bit because it outweighs the public's interest in a speedy trial, and Mr. Chatrie's, given the weight and the seriousness of the issues before me.

But I do tell you all that we are on it, and I am aware that, especially with COVID and with folks being unable to travel from California to testify in person, that this is an unusually long pendency in a case, and I am taking that into account as I approach it. All right?

Is there anything else I need to cover?

MR. SIMON: Nothing further, Judge.

MS. KOENIG: Not from the defense, Your Honor. Thank you.

THE COURT: All right. Well, you all have done a tremendous job. And thank you for your time, and I will issue my opinion. Thank you.

(The proceedings were adjourned at 3:00 p.m.)

I, Diane J. Daffron, certify that the foregoing is

a correct transcript from the record of proceedings in the above-entitled matter.

/s/

DIANE J. DAFFRON, RPR, CCR DATE